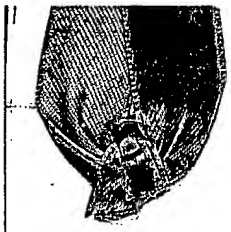


日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

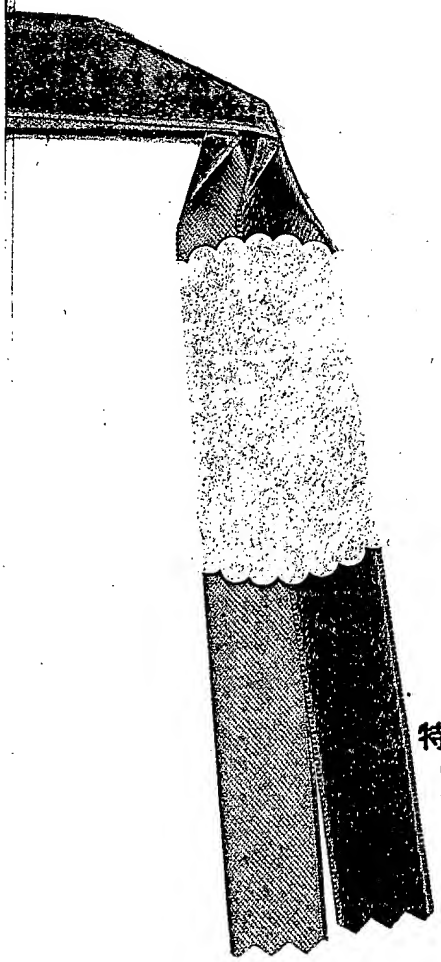
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　１月１３日

出 願 番 号
Application Number: 特願２０００－００４２７２

出 願 人
Applicant (s): カシオ計算機株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　４月　７日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号　出証特２０００－３０２４１７９

【書類名】　特許願

【整理番号】　99-2068-00

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

G06F 12/14

【発明者】

【住所又は居所】　東京都羽村市栄町３丁目２番１号

カシオ計算機株式会社羽村技術センター内

【氏名】　大塚　基

【特許出願人】

【識別番号】　000001443

【氏名又は名称】　カシオ計算機株式会社

【代理人】

【識別番号】　100074985

【弁理士】

【氏名又は名称】　杉村　次郎

【手数料の表示】

【予納台帳番号】　023180

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9109737

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】セキュリティ管理システムおよびそのプログラム記録媒体

【特許請求の範囲】

【請求項１】

携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、

サーバ装置は、携帯端末装置との対応付けが設定されている可搬型データ記憶媒体に配布すべきデータファイルの各レコードを個別に暗号化する暗号化手段と、

この暗号化手段によって各レコードが個別に暗号化されたデータファイルを当該データ記憶媒体に書き込む書込手段とを具備し、

携帯端末装置は、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体かを判別する判別手段と、

この判別手段によって端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のデータファイルへのアクセスを許可するアクセス制御手段と、

このアクセス制御手段によってデータ記憶媒体内のデータファイルへのアクセスが許可された場合に、アクセス対象として任意に指定されたレコードを個別に読み込み、この読み込んだレコードを処理対象としてその復号化処理と復号化されたレコード内容を表示するレコード出力処理を実行するレコード処理手段とを具備したことを特徴とするセキュリティ管理システム。

【請求項２】

前記レコード処理手段は、復号化処理によって復号化されたレコード内容を端末内の一時記憶メモリに記憶させ、前記データファイルに対するアクセス処理の終了あるいはその端末処理終了により、前記一時記憶メモリ内の復号化レコードを消去するようにしたことを特徴とする請求項1記載のセキュリティ管理システム。

【請求項３】

前記暗号化手段は、データファイルの各レコードを個別に暗号化すると共に、そのレコード内の各フィールドを個別に暗号化し、

前記レコード処理手段は、データ記憶媒体内のデータファイルをアクセスする際に、アクセス対象として任意に入力されたキーを暗号化すると共に、暗号化されているデータファイルの各レコードを前記暗号化されたキーに基づいて検索することにより、入力キーに該当するフィールドを持つレコードを個別に読み込み、この読み込んだレコードを処理対象としてその復号化処理と復号化されたレコード内容を表示するレコード出力処理を実行するようにしたことを特徴とする請求項1記載のセキュリティ管理システム。

【請求項４】

前記レコード処理手段は、データ記憶媒体内のデータファイルから個別に読み込んでそれを復号化したレコードに対してその変更が指示されたり、当該データファイルに対して新規レコードの追加が指示された場合に、その変更されたレコードあるいは追加されたレコードを暗号化すると共に、暗号化されたレコードを前記データファイルに対する更新情報としてデータ記憶媒体内に書き込むようにしたことを特徴とする請求項1記載のセキュリティ管理システム。

【請求項５】

コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、

サーバ装置に対して、携帯端末装置との対応付けが設定されている可搬型データ記憶媒体に配布すべきデータファイルの各レコードを個別に暗号化させるコンピュータが読み取り可能なプログラムコードと、

各レコードが個別に暗号化されたデータファイルを当該データ記憶媒体に書き込ませるコンピュータが読み取り可能なプログラムコードと、

携帯端末装置に対して、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体かを判別させるコンピュータが読み取り可能なプログラムコードと、

端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のデータファイルへのアクセスを許可させるコンピュータが読み取り可能なプログラムコードと、

データ記憶媒体内のデータファイルへのアクセスが許可された場合に、アクセス対象として任意に指定されたレコードを個別に読み込み、この読み込んだレコ

ードを処理対象としてその復号化処理と復号化されたレコード内容を表示するレコード出力処理を実行させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、携帯端末装置によって可搬型データ記憶媒体をアクセスする際のセキュリティ対策を講じたセキュリティ管理システムおよびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】

近年、コンパクトディスクやメモリカード等の可搬型記憶媒体は、大容量化、小型化が進み、大量のデータベースを可搬型記憶媒体に格納することによって、各種のデータベースを自由に持ち運びことができるようになってきている。ここで、営業担当者が携帯端末装置を持参して、日常の営業活動を行う場合において、携帯端末装置はその内蔵メモリの容量が少ないために、各種業務処理用のデータベースの一部あるいは全部を可搬型記憶媒体に格納するようにしている。ここで、営業担当者は、端末本体に可搬型記憶媒体を装着し、外出先でその記憶内容をアクセスして表示出力させたり、データ更新等を行うようにしている。この場合、携帯端末装置によって可搬型データ記憶媒体をアクセスする際のセキュリティ対策としては、入力されたパスワードによって正当な端末利用者かを認証するようにしている。

【０００３】

【発明が解決しようとする課題】

ところで、本来、個人専用機としての携帯端末装置においても、正社員の他、派遣社員、パート、アルバイトの方も使用するケースが増えてきている。また、携帯端末装置は、外出先に持ち運んで使用するという関係上、可搬型記憶媒体や携帯端末装置自体を外出先で紛失したり、盗難される危険性があった。したがって、可搬型記憶媒体や端末の内蔵メモリ内に、機密性の高い重要な企業情報や個

人情報が格納されている場合に、紛失、盗難、悪意によって、その重要情報が他人に漏洩されるおそれは極めて高かった。

すなわち、従来においては、携帯端末装置を主に外出先で使用するという関係上、入力操作を複雑化した厳密なセキュリティ管理よりも、操作の簡素化、迅速性等の操作環境を重視しているため、可搬型記憶媒体や携帯端末装置の紛失や盗難に対するセキュリティ対策や派遣社員、パート等による悪意に対するセキュリティ対策は、十分ではなく、ユーザパスワードを知っていれば、あるいはパスワードの偶発的なヒットによって、誰でも、どのパソコンからでも容易に携帯端末や記憶媒体内のデータをアクセスすることができ、重要情報が他人に漏洩されてしまう危険性は、極めて高かった。また、ユーザ設定によって、任意にセキュリティ対策を講じるための仕組みを携帯端末装置自体に持たせておくことは、逆に、第３者によってその設定部分の変更も容易に行える危険性を含むことになり、その仕組み自体が安全性を損なう要因となってしまう。

この発明の課題は、可搬型データ記憶媒体内のデータファイルを各レコード毎に暗号化しておくことで、当該記憶媒体をアクセスする場合でも、暗号化されたままの状態で行うことができ、記憶媒体の紛失、盗難あるいは悪意等において、仮に、正当な端末以外がデータファイルのアクセスまでたどり着いた最悪のケースでも、復号化されたレコードのみのセキュリティが問題になるだけで、そのファイルの全貌が解読される危険性はなく、重要情報の漏洩を確実に防止できるようにすることである。

【０００４】

この発明の手段は、次の通りである。

請求項第１記載の発明は、携帯端末装置と、この携帯端末装置によって利用される可搬型データ記憶媒体にデータファイルを書き込んで配布するサーバ装置とを有し、サーバ装置は、携帯端末装置との対応付けが設定されている可搬型データ記憶媒体に配布すべきデータファイルの各レコードを個別に暗号化する暗号化手段と、この暗号化手段によって各レコードが個別に暗号化されたデータファイルを当該データ記憶媒体に書き込む書込手段とを具備し、携帯端末装置は、それにセットされているデータ記憶媒体が当該端末に対応付けられている正当な媒体

かを判別する判別手段と、この判別手段によって端末対応の媒体であることが判別された場合に、そのデータ記憶媒体内のデータファイルへのアクセスを許可するアクセス制御手段と、このアクセス制御手段によってデータ記憶媒体内のデータファイルへのアクセスが許可された場合に、アクセス対象として任意に指定されたレコードを個別に読み込み、この読み込んだレコードを処理対象としてその復号化処理と復号化されたレコード内容を表示するレコード出力処理を実行するレコード処理手段とを具備するものである。

なお、この発明は次のようなものであってもよい。

（１）前記レコード処理手段は、復号化処理によって復号化されたレコード内容を端末内の一時記憶メモリに記憶させ、前記データファイルに対するアクセス処理の終了あるいはその端末処理終了により、前記一時記憶メモリ内の復号化レコードを消去する。

（２）前記暗号化手段は、データファイルの各レコードを個別に暗号化すると共に、そのレコード内の各フィールドを個別に暗号化し、前記レコード処理手段は、データ記憶媒体内のデータファイルをアクセスする際に、アクセス対象として任意に入力されたキーを暗号化すると共に、暗号化されているデータファイルの各レコードを前記暗号化されたキーに基づいて検索することにより、入力キーに該当するフィールドを持つレコードを個別に読み込み、この読み込んだレコードを処理対象としてその復号化処理と復号化されたレコード内容を表示するレコード出力処理を実行する。

（３）前記レコード処理手段は、データ記憶媒体内のデータファイルから個別に読み込んでそれを復号化したレコードに対してその変更が指示されたり、当該データファイルに対して新規レコードの追加が指示された場合に、その変更されたレコードあるいは追加されたレコードを暗号化すると共に、暗号化されたレコードを前記データファイルに対する更新情報としてデータ記憶媒体内に書き込む。

したがって、請求項第１記載の発明においては、可搬型データ記憶媒体内のデータファイルを各レコード毎に暗号化しておくことで、当該記憶媒体をアクセスする場合でも、暗号化されたままの状態で行うことができ、記憶媒体の紛失、盗

難あるいは悪意等において、仮に、正当な端末以外がデータファイルのアクセスまでたどり着いた最悪のケースでも、復号化されたレコードのみのセキュリティが問題になるだけで、そのファイルの全貌が解読される危険性はなく、重要情報の漏洩を確実に防止することができる。

【０００５】

【発明の実施の形態】

以下、図１～図１７を参照してこの発明の一実施形態を説明する。

図１は、この実施形態におけるセキュリティ管理システムの全体構成を示したブロック図である。

このセキュリティ管理システムは、例えば、会社組織において会社側に設置させているサーバ装置１と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末装置）２と、この携帯端末装置２にセットされて利用される可搬型記憶媒体３とを有している。そして、サーバ装置１側で記憶管理されているアプリケーションソフト／データベース等を持ち運び自在な可搬型記憶媒体３を介して携帯端末装置２側に外部提供するようにしており、この記憶媒体３にデータベース等を書き込んで端末装置へ配布する際に、サーバ装置１は当該端末と記憶媒体とを対応付けるための情報を設定したり、各種のセキュリティ対策を講じることによって、記憶媒体３内のアプリケーションソフト／データベース等が第三者によって不正コピーされたり、情報が漏洩されることを確実に防止するようにしたものである。

【０００６】

そして、各営業担当者は、外出先で可搬型記憶媒体３内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記憶媒体３を抜き取り、それをサーバ装置１側のカードリーダ／ライタ４にセツトすると、サーバ装置１はカードリーダ／ライタ４を介して記憶媒体３内の営業記録を収集処理するようにしている。

そして、サーバ装置１と複数台の携帯端末装置２とはシリアルケーブル５を介して着脱自在に接続可能となっている。

【０００７】

可搬型記憶媒体３は、各種業務処理用のアプリケーションソフトやデータベース等を記憶するもので、例えば、コンパクトフラッシュカードによって構成されている。以下、可搬型記憶媒体３をモバイルデータベースカード（ＤＢカード）と称する。ここで、図中、各ＤＢカード３に付した「＃Ａ」「＃Ｂ」、「＃Ｃ」、‥‥は、端末名称「Ａ」、「Ｂ」、「Ｃ」、‥‥で示される携帯端末装置２に対応付けられた端末対応のカードであることを示している。なお、この実施形態においては端末対応のカードの他、後述する端末グループ対応のカードも存在するが、図１の例では端末対応のカードのみを示している。カードリーダ／ライタ４はＤＢカード３を複数枚同時にセット可能なもので、複数のカード挿入口を有している。

そして、サーバ装置１はＤＢカード３を介して携帯端末装置２側にアプリケーションソフト／データベースファイル（ＡＰソフト／ＤＢファイル）を配布する。すなわち、サーバ装置１はＤＢカード３に書き込む書込対象、つまり、配布対象のＡＰソフト／ＤＢファイルを呼び出してカードリーダ／ライタ４に与え、それにセットされている１または２以上のＤＢカード３にＡＰソフト／ＤＢファイルを書き込む。

【０００８】

図２は、例えば、業務グループ「営業１課」、「営業２課」、「プロジェクトＡ」、「プロジェクトＢ」、‥‥に対応付けた端末グループと、この端末グループ対応のＤＢカード３との関係を示すと共に、端末とユーザとの対応関係を示したものである。すなわち、図中、「＃Ａ１」、「＃Ａ２」、「＃Ａ３」で示す各ＤＢカード３は、端末名称が「Ａ１」、「Ａ２」、「Ａ３」である各携帯端末装置２が属する端末グループＡ対応の記憶媒体であり、同様に、「＃Ｂ１」、「＃Ｂ２」‥‥で示す各ＤＢカード３は、端末名称が「Ｂ１」、「Ｂ２」、‥‥である各携帯端末装置２が属する端末グループＢ対応の記憶媒体であり、同一グループ内の各ＤＢカード３はそのグループに属する各携帯端末装置２で共通して使用することができるようになっている。

【０００９】

また、ある携帯端末を利用することができる権限を有するユーザは、一人と限

らず、複数のユーザが一台の携帯端末装置を共有して使用することができ、また、あるユーザは複数台の携帯端末装置を利用することができる権限を有している。例えば、端末グループＡにおいて、端末名称「Ａ１」で示される携帯端末装置と、ユーザ「ＵＡ１」～「ＵＡ４」との対応関係が定義され、また、端末名称「Ａ２」で示される携帯端末装置と、ユーザ「ＵＡ１」～「ＵＡ３」との対応関係が定義されており、これらの間に限り利用関係があることを示している。この場合、複数ユーザによる共有使用が可能な端末対応の各ＤＢカードには、共有使用が可能な各ユーザに対応して、その認証情報（パスワード）が設定される。

【００１０】

図３は、この実施形態の特徴である多重セキュリティ管理の仕組みを概念的に示した図である。この多重セキュリティ管理は、携帯端末装置２が任意のＤＢカードをアクセスする際、あるいはＤＢカード３が任意の端末装置によってアクセスされる際のセキュリティ処理を示したもので、この多重セキュリティを大別すると、４つのセキュリティ層からなる。

すなわち、この多重セキュリティ管理の仕組みは、第１セキュリティ層（ＤＢカードセキュリティ）と、第２セキュリティ層（パスワード認証）と、第３セキュリティ層（ソフトセキュリティ）と、第４セキュリティ層（データベース多重暗号化）とから成っている。

【００１１】

第１セキュリティ層（ＤＢカードセキュリティ）は、携帯端末装置２が任意のＤＢカードをアクセスする際に、あるいはＤＢカード３が任意の端末装置によってアクセスされる際において、端末およびカード内にそれぞれ記憶されている第１の識別情報（後述するハード識別番号）同士を照合し、その照合結果に基づいて当該カード自体に対するアクセス可否を決定するチェック処理である。このチェック処理は端末の電源投入時において、カード内に格納されている基本ソフトの起動によって実行開始される。

【００１２】

ここで、「ハード識別番号」は、携帯端末装置２とＤＢカード３とを対応付けておくために予め携帯端末装置２やＤＢカード３に書き込まれたものである。す

なわち、サーバ装置１が携帯端末装置２やＤＢカード３へ書き込むための内容を予めテーブル設定しておく際に、「ハード識別番号」は、同一グループに属する携帯端末装置２のうち、いずれか一台の端末から読み込んだ固有の端末識別情報（製造番号）に応じて生成されたもので、サーバ装置１はグループ対応の各携帯端末装置２およびそれらの端末で利用される各ＤＢカード３内に、ハード識別番号をそれぞれ書き込む。したがって、同一グループに属する各携帯端末装置２および各ＤＢカード３内には、それぞれ同一のハード識別番号が共通のアクセス制限情報としてそれぞれ書き込まれる。

【００１３】

第２セキュリティ層（パスワード認証）は、上述のＤＢカードセキュリティチェックの結果、当該カード自体に対するアクセスが許可された場合に、入力されたユーザ認証情報（パスワード）に基づいて正当なオペレータかを照合するチェック処理である。

この場合の照合には、暗号化パスワードが用いられる。すなわち、この暗号化パスワードは、入力されたパスワードを所定の方法で暗号化したもので、端末対応の各ＤＢカード３内にユーザ固有の認証情報としてそれぞれ書き込まれる。この場合、その端末に対してアクセス権限が付与されている複数のユーザが存在している場合には、各ユーザ毎に暗号化パスワードの書き込みが行われる。

【００１４】

なお、この第２セキュリティ層においては、ＤＢカード３の利用時において、ユーザパスワードが入力された際に、間違ったパスワードが連続して何回か繰り返して誤入力された場合、その繰り返し入力回数が予め設定されている限度値（後述するビューア不作動設定回数）に達したことが判別されると、それ以降、検索ビューア（パスワード入力を促す表示等の初期画面表示）を不作動とすることにより、パスワード入力を受け付けない状態とするセキュリティ処理も合わせて行うようにしている。

【００１５】

第３セキュリティ層（ソフトセキュリティ）は、携帯端末装置２が任意のＤＢカードをアクセスする際に、あるいはＤＢカード３が任意の端末装置によってア

クセスされる際において、端末およびカード内にそれぞれ記憶されている第２の識別情報（後述するソフト識別番号）同士を照合し、その照合結果に基づいて当該カード内のデータベース（モバイルＤＢ）に対するアクセス可否を決定するチェック処理である。

この「ソフト識別番号」は、ＤＢカード３内のデータベースと、それを利用可能な携帯端末装置２とを対応付けておくために予め携帯端末装置２やＤＢカード３に書き込まれたものである。すなわち、サーバ装置１が携帯端末装置２やＤＢカード３へ書き込むための内容を予めテーブル設定しておく際に、「ソフト識別番号」は、同一グループに属する携帯端末装置２のうち、そのいずれか一台の端末から読み込んだ固有の端末識別情報（製造番号）と、そのグループ名称、所定のマスタＤＢ名に応じて生成されたもので、サーバ装置１はグループ対応の各携帯端末装置２およびそれらの端末に対応付けられている各ＤＢカード３内に、ソフト識別番号をそれぞれ書き込む。

【００１６】

第４セキュリティ層（データベース多重暗号化）は、ＤＢカードを紛失したり、盗難されたような場合に、仮に、第三者がそのＤＢカードに対してアクセスすることができたとしても、ＤＢカード内のデータベースを多重暗号化によってその解読を防止するセキュリティ対策を示している。

ここで、サーバ装置１はＤＢカード３にデータベースを書き込んで配布する際に、配布先のグループに対応付けられているマスタデータベースをそのままカードに書き込むのではなく、マスタデータベースから当該グループの業務内容に応じて必要なデータ内容のみを切り出し、切り出したデータからなるグループ対応のデータベース（モバイルＤＢ）を作成するようにしているが、その際、作成されたモバイルＤＢのファイル管理情報、つまり、各ファイルの格納位置を示すＦＡＴ（Ｆｉｌｅ・Ａｌｌｏｃａｔｉｏｎ・Ｔａｂｌｅ）をスクランブル処理（暗号化処理）するようにしている。

このＦＡＴスクランブル処理は、スクランブル処理用として任意に生成された暗号キー（スクランブルキー）を用いて行われるが、スクランブル処理をどのような手法で行うかは、任意である。

また、サーバ装置１はＤＢカード３内にモバイルＤＢを書き込む際に、任意に生成したレコード暗号化キーを用いて１レコード、フィールド毎にモバイルＤＢの各レコードを個別に暗号化するようにしている。このようにモバイルＤＢは多重暗号化されてＤＢカード内に書き込まれる。

【００１７】

図４（Ａ）は、サーバ装置１側に設けられている設定テーブル１１を示している。この設定テーブル１１はサーバ装置１がＤＢカード３や携帯端末装置２に書き込むための各種の内容を予め設定しておくもので、この実施形態においては、ＤＢカード３への書き込みを携帯端末装置２自体に行わせるのではなく、サーバ装置１が一括して行うようにしている。

設定テーブル１１はグループ「営業１課」、「営業２課」、「プロジェクトＡ」、「プロジェクトＢ」、‥‥のような端末グループ毎に、各種の設定エリアを有する構成となっている。この各グループ毎の設定エリアにセットされた内容は、当該グループ対応の各携帯端末装置２や各ＤＢカード３内に書き込まれる。なお、図４（Ａ）は、端末グループとして「営業１課」、「営業２課」、「営業１課」を例示した場合を示している。

先ず、各グループ対応の設定エリアには「グループ名称」の他、上述した「ハード識別番号」、同一グループに属する端末の合計「設定台数」、その各端末毎の「端末名（１）、端末名（２）、‥‥」、同一グループ内のおいて、その端末を使用することができる権限を持つユーザの合計「使用人数」がぞれぞれ設定されている。

【００１８】

更に、グループ毎に設定されている「ビューア不作動設定回数（Ｎ）」は、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするためにグループ毎に任意に設定された設定回数である。

また、使用の権限を有する各ユーザに対応付けて、その「ユーザ名（１）」、「パスワード」、「ユーザ名（２）」、‥‥が設定されている。また、グループ毎に上述した「スクランブルキー（ＳＫ）」、「レコード暗号化キー（ＲＫ）」がそれぞれ設定されている。

【００１９】

また、書き込み対象としての各データベースに対応付けて、その「モバイルＢＤ名（１）」、「マスタＤＢ名」、「レコード抽出条件」、「抽出対象フィールド」、「モバイルＢＤ名（２）」‥‥が設定されている。

「マスタＤＢ名」は、図４（Ｂ）で示すように、サーバ装置側で記憶管理されている複数のマスタＤＢファイル１２のうち、当該グループの業務内容等に応じて必要とするマスタＤＢを指定するものであり、また、「レコード抽出条件」、「抽出対象フィールド」は、そのマスタＤＢを当該グループの業務内容等に応じて修正変更することによってグループ対応のモバイルＢＤを作成する際に使用されるモバイルＢＤ作成用の条件を定義するものである。

すなわち、「レコード抽出条件」はこのマスタＤＢから所望するレコード群を抽出するための抽出条件を示し、「抽出対象フィールド」はこの抽出レコード群から所望するフィールドのみからなるレコード構成に変更するためのフィールド抽出条件を示している。そして、「レコード抽出条件」、「抽出対象フィールド」をマスタＢＤ毎に設定しておくことにより、当該グループの業務内容や携帯端末毎の処理内容にマッチした固有のモバイルＢＤが作成される。

【００２０】

また、「モバイルＤＢ名（１）」、「モバイルＤＢ名（２）」‥‥に対応付けて「カスタマイズＡＰ（１）」、「カスタマイズＡＰ（２）」‥‥が設定されている。この「カスタマイズＡＰ」は上述のモバイルＢＤを処理するためのアプリケーションソフトであり、マスタＤＢ対応の基本ＡＰ１３（図４（Ｃ）参照）をモバイルＢＤに応じてその表示形態を修正変更したものである。

この「対応カスタマイズＡＰ」には上述した「ソフト識別番号」、「更新日付」、「対応モバイルＤＢ名」が対応設定されている。この場合、「ソフト識別番号」は同一グループ内の各「カスタマイズＡＰ」に共通して設定されるが、「更新日付」はその基本ＡＰを修正変更した時の日によって相違する。

なお、「カスタマイズＡＰ」の設定エリアに、そのＡＰ名だけをセットするようにしてもよい。この場合には、当該カスタマイズＡＰ自体は別ファイルに格納しておき、設定テーブル１１内の対応カスタマイズＡＰ名に応じて当該アプリ

ケーションソフト自体を呼び出すようにしてもよい。

【００２１】

一方、設定テーブル１１には、各グループに共通して各ＤＢカードに書き込まれる共通の書き込み対象として、「基本ソフト」がグループ対応設定エリアとは別のエリアに設定されている。ここで、「基本ソフト」には「検索ビューア」、「ＦＡＴスクランブル／解除アルゴリズム」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」を含む構成となっている。

「基本ソフト」は、携帯端末装置の基本的な動作を実行制御するための基本ソフトであり、「検索ビューア」は基本ソフトの動作に応じて初期画面（ログイン入力画面）を表示させるソフトである。「動作制御管理ファイル」はＤＢ対応カスタマイズＡＰを動作制御するための基本的な管理情報が格納されているファイルである。この「動作制御管理ファイル」は通常カード内に書き込まれているが、この実施形態においては、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビューアを不作動とするために、「動作制御管理ファイル」を削除するようにしており、検索ビューア起動時に、この「動作制御管理ファイル」がＤＢカード内に存在していることを条件として、携帯端末装置はログイン入力画面を表示させるようにしている。

【００２２】

図５は、サーバ装置によって各ＤＢカード３に書き込まれた内容を示している。すなわち、ＤＢカードには、「ハード識別番号」、「ＦＡＴ（スクランブル済み）」、「基本ソフト」、「検索ビューア」、「ＦＡＴスクランブル／解除アルゴリズム」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」、「ビューア不作動設定回数」が書き込まれている。「ＦＡＴ（スクランブル済み）」は当該ＤＢカード内の各モバイルＤＢを管理する管理情報であり、スクランブル処理された内容のまま書き込まれている。

更に、当該ＤＢカードを使用可能な各ユーザに対応して「ユーザ名（１）」、「暗号化パスワード＋時間変数キー」、「ユーザ名（２）」‥‥が書き込まれていると共に、「レコード暗号化キー（ＲＫ）」が書き込まれている。

また、「モバイルＤＢ名（１）」、その実データである「ＤＢ（暗号済み）

」、「モバイルＤＢ名（２）」‥‥が書き込まれ、更にモバイルＤＢに対応付けて「カスタマイズＡＰ（１）」と、「ソフト識別番号」、「更新日付」、「対応モバイルＤＢ名」、「カスタマイズＡＰ（２）」‥‥が書き込まれている。

【００２３】

図６は、各携帯端末装置２の内蔵メモリに書き込まれた内容を示している。この内蔵メモリには、図示のようにフラッシュＲＯＭ、ＲＡＭ（一時記憶メモリ）が設けられている。このＲＯＭ、ＲＡＭは、セキュリティ対策をも考慮して必要最小限のメモリ容量とした構成となっている。すなわち、この実施形態においては、上述のように、アプリケーション、データベース、基本ソフト等の格納場所を携帯端末装置２とＤＢカード３とに分散せず、ＤＢカード３にアプリケーション、データベースの他、基本ソフトをも書き込むようにしており、携帯端末自体の紛失、盗難等によるリスクを解消できるようにしている。

ここで、サーバ装置１の書き込み動作によって端末内のフラッシュＲＯＭには、上述した「ハード識別番号」、「ソフト識別番号」、「スクランブルキー（ＳＫ）」が固定的に記憶される。また、一時記憶メモリであるＲＡＭは、「キー／データ入力エリア」、「ＦＡＴ読み出しエリア」、「レコードエリア」、「その他のワークエリア」を有する構成となっている。なお、「レコードエリア」は端末内にデータを残さないようにするため、必要最小限のデータ、つまり、現在処理中のカレント分として１レコード分のデータを一時記憶する構成となっている。　なお、図示しないが、各携帯端末装置２の内部メモリには、それが製造された端末固有の製造番号も固定的に記憶されている。

【００２４】

図７は、サーバ装置１、携帯端末装置２の全体構成を示したブロック図である。

ここで、サーバ装置１、携帯端末装置２の構成要素として基本的に同様なものは、同一番号を付してその説明を兼用するが、サーバ装置１、携帯端末装置２との構成要素を識別するために、サーバ装置１の構成要素には、図中「Ａ」を付し、以下、携帯端末装置２の構成のみを説明し、サーバ装置１の説明は省略するものとする。

ＣＰＵ２１は、記憶装置２２内のオペレーティングシステムや各種アプリケーションソフトにしたがってこの携帯端末装置２の全体動作を制御する中央演算処理装置である。記憶装置２２は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁気的、光学的、半導体メモリ等によって構成されている記録媒体２３やその駆動系を有している。この記録媒体２３はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なＣＤ－ＲＯＭ、フロッピィデスク、ＲＡＭカード、磁気カード等の可搬型の媒体である。また、この記録媒体２３内のプログラムやデータは、必要に応じてＣＰＵ２１の制御によりＲＡＭ（例えば、スタティクＲＡＭ）２４にロードされたり、ＲＡＭ２４内のデータが記録媒体２３にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、ＣＰＵ21は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。

また、ＣＰＵ２１は記録媒体２３内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体２３に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウエーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部２５によって受信して記録媒体２３内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、ＣＰＵ２１は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。

一方、ＣＰＵ２１にはその入出力周辺デバイスである伝送制御部２５、入力部２６、表示部２７がバスラインを介して接続されており、入出力プログラムにしたがってＣＰＵ２１はそれらの動作を制御する。入力部２６はキーボードやタッチパネルあるいはマウスやタッチ入力ペン等のポインティングデバイスを構成する操作部であり、文字列データや各種コマンドを入力する。

【００２５】

次に、この一実施形態におけるセキュリティ管理システムの動作を図８～図

１１および図１３～図１７に示すフローチャートを参照して説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記録媒体２３（２３Ａ）に格納されており、ＣＰＵ２１（２１Ａ）はこのプログラムコードにしたがった動作を逐次実行する。また、ＣＰＵ２１（２１Ａ）は伝送媒体を介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【００２６】

図８および図９は、サーバ装置１が設定テーブル１１に対して各種設定を行う場合の動作を示したフローチャートである。

先ず、基本的なグループ情報を設定登録する処理が行われる（ステップＡ１～Ａ１０）。ここで、オペレータは入力可能な状態において、今回設定する１グループ分の「グループ名称」を入力指定すると共に（ステップＡ１）、そのグループ内の端末「設定台数」、ユーザ「使用人数」の入力を行う（ステップＡ２）。そして、指定台数分の携帯端末装置２と、その端末に対応付けるＤＢカード３とをサーバ装置１にセットした後（ステップＡ３）、セットした台数分の「端末名」をそれぞれ入力する（ステップＡ４）。

【００２７】

すると、サーバ装置１はセットされている同一グループ内の各端末のうち、いずれか１台の端末を選択指定して、その「製造番号」を読み出すと共に（ステップＡ５）、この「製造番号」に基づいて「ハード識別番号」を生成して（ステップＡ６）、設定台数分の各携帯端末装置２およびＤＢカード３に「ハード識別番号」をそれぞれ書き込む（ステップＡ７）。なお、テーブル設定時において、携帯端末装置／ＤＢカードへの書き込みは、「ハード識別番号」の生成時と後述する「ソフト識別番号」生成時および「スクランブルキー（ＳＫ）」の生成時の場合に限り行うようにしている。

次のステップＡ８では、上述のように入力された「グループ名称」、「設定台数」、「端末名」、「使用人数」の他、生成した「ハード識別番号」を設定テー

ブル１１にそれぞれ登録する処理が行われる。

そして、パスワード不一致でのビューア不作動回数として任意の値をオペレータが入力すると（ステップＡ９）、入力された「ビューア不作動回数」は、設定テーブル１１に登録される（ステップＡ１０）。

【００２８】

このようにしてグループ基本情報の設定登録が終わると、そのグループの使用人数分のパスワードを設定登録する処理に移る（ステップＡ１１～Ａ１５）。

先ず、オペレータはユーザ名を入力すると共に（ステップＡ１）、そのユーザ対応のパスワードを入力すると（ステップＡ１２）、入力されたユーザ名、パスワードは設定テーブル１１にそれぞれ登録される（ステップＡ１３）。これによって一人分のユーザ登録が終わると、使用人数分のユーザ登録が終了したかを調べ（ステップＡ１４）、全ユーザ分の設定が終了するまで上述の動作を繰り返す。

【００２９】

そして、ユーザ登録が終了すると、次に、「スクランブルキー（ＳＫ）」、「レコード暗号化キー（ＲＫ）」を設定登録する処理に移る（ステップＡ１５～Ａ１７）。

先ず、「スクランブルキー（ＳＫ）」を生成すると共に（ステップＡ１５）、「レコード暗号化キー（ＲＫ）」を生成する（ステップＡ１６）。この「スクランブルキー（ＳＫ）」は上述したように、モバイルＤＢのＦＡＴをスクランブル処理する際に使用される暗号キーであり、また、「レコード暗号化キー（ＲＫ）」は、データベースを１レコード、フィルード毎に暗号化する際に使用される暗号化キーである。この場合のキー生成方法は、任意であり、その都度、ランダムに生成するようにしてもよい。

そして、生成した「スクランブルキー（ＳＫ）」、「レコード暗号化キー（ＲＫ）」を設定テーブル１１にそれぞれ登録すると共に（ステップＡ１７）、生成した「スクランブルキー（ＳＫ）」を設定台数分、各携帯端末装置２にそれぞれ書き込む（ステップＡ１８）。

【００３０】

次に、データベースおよびそれに対応するアプリケーションソフトを設定登録する処理に移る（図９のステップＡ２０～Ａ３４）。

先ず、オペレータはＤＢカードに書き込むための「モバイルＤＢ名」およびその作成の元となる「マスタＤＢ名」を指定入力すると（ステップＡ２０、Ａ２１）、この「モバイルＤＢ名」と共に「マスタＤＢ名」は、設定テーブル１１に対応して登録される（ステップＡ２２）。そして、指定されたマスタＤＢにおけるファイルのレコード構成が案内表示される（ステップＡ２３）。すなわち、マスタＤＢの各レコードが図１２（Ａ）に示すように８フィールド「Ａ」、「Ｂ」～「Ｈ」の各項目から構成されているものとすると、この１レコード分の各項目名がその並び順に案内表示される。

【００３１】

ここで、オペレータはレコード構成の案内表示を確認し、「レコード抽出条件」を指定入力する（ステップＡ２４）。つまり、案内表示されているレコード構成の各フィールドうち、所望するフィールドを条件設定対象フィールドとして指定した後、その指定フィールドに対する「レコード抽出条件」を指定入力する。例えば、更新日付の項目を条件設定対象フィールドとして指定した後、１９９９年12月２４日以降に更新されたレコードを「レコード抽出条件」として指定する。次に、レコード構成の対象とするフィールドを選択指定する（ステップＡ２５）。例えば、案内表示されているレコード構成の各フィールドうち、所望するフィールドを「抽出対象フィールド」として選択指定する。すると、指定入力された「レコード抽出条件」およびレコード構成の「対象フィールド名」が当該モバイルＤＢ名に対応して設定テーブル１１にそれぞれ登録される（ステップＡ２６）。

そして、当該グループで使用する書き込み対象としての全てのモバイルＤＢを指定し終わったかを調べ（ステップＡ２７）、全ての指定が終わるまで、上述の動作を繰り返すことにより、モバイルＤＢの設定登録を行う（ステップＡ２０～Ａ２７）。

【００３２】

これによって、モバイルＤＢの設定登録が終わると、上述のようにして読み込

んだ「製造番号」と、当該グループ内において最初に指定された「モバイルＤＢ名」と、入力された「グループ名」とに基づいて「ソフト識別番号」を生成すると共に（ステップＡ２８）、この「ソフト識別番号」を設定台数分の携帯端末装置２にそれぞれ書き込む（ステップＡ２９）。

次に、今回設定登録した各モバイルＤＢ名に対応付けてそのカスタマイズＡＰを設定登録する処理に移る。すなわち、設定登録した各モバイルＤＢ名のうち、そのいずれかをオペレータが指定すると（ステップＡ３０）、指定されたモバイルＤＢ名に対応する「マスタＤＢ名」が読み出され、このマスタＤＢ対応の基本ＡＰ１３をアクセスし、当該モバイルＤＢを利用するための表示形態に、この基本ＡＰを修正変更することにより、所望するカスタマイズＡＰを任意に作成する（ステップＡ３１）。

【００３３】

例えば、当該モバイルＤＢのレコード構成に応じてどのフィールドをどの位置に表示させるかを指定したり、各フィールドの表示サイズ等を任意に指定しながら基本ＡＰを修正変更することにより、所望するカスタマイズＡＰを作成する。

そして、作成したカスタマイズＡＰに「ソフト識別番号」、現在のシステム日付である「更新日付」、「対応モバイルＤＢ名」を書き込んだ後（ステップＡ３２）、このカスタマイズＡＰを設定テーブル１１に登録する（ステップＡ３３）。そして、全てのカスタマイズＡＰを作成登録し終わるまで（ステップＡ３４）、上述の動作を繰り返す（ステップＡ３０～Ａ３４）。

【００３４】

次に、全てのグループに対する設定登録が終了したかを調べ（ステップＡ３５）、全グループ終了が判別されるまでステップＡ１に戻り、１グループ毎に上述の動作を繰り返す。これによって設定テーブル１１には、各グループに対応して図４に示した各種の内容が設定登録される。その際、１グループ分の設定登録が終了する毎に、次の設定対象グループを指定して、そのグループ対応の携帯端末装置２、ＤＢカード３をサーバ装置１にセットする。このようなテーブル設定によって携帯端末装置２には「ハード識別番号」、「ソフト識別番号」、「スクランブルキー（ＳＫ）」がそれぞれ書き込まれ、更に、ＤＢカード３には「ハード

識別番号」、「ソフト識別番号」がそれぞれ書き込まれる。

【００３５】

図１０および図１１は、サーバ装置１がモバイルＤＢや対応カスタマイズＡＰ等をＤＢカード３に書き込んで配布する場合の動作を示したフローチャートである。

先ず、オペレータはサーバ装置１に配布対象の１または２以上のＤＢカード３をセットする（ステップＢ１）。すると、セットされているＤＢカードの中から１つのカードを選択して、そのカード内から「ハード識別番号」を読み出すと共に（ステップＢ２）、このハード識別番号に基づいて設定テーブル１１を検索し、該当するグループを特定しておく（ステップＢ３）。

そして、各グループに共通して各ＤＢカードに書き込まれる共通の書き込み対象としての「基本ソフト」を設定テーブル１１から読み出し、そのＤＢカードに書き込む（ステップＢ４）。この場合、「基本ソフト」には「検索ビューア」、「ＦＡＴスクランブル／解除アルゴリズム」、「暗号化／復号化アルゴリズム」、「動作制御管理ファイル」が含まれているので、それらを含めて書き込まれる。

次に、特定したグループ対応の「ビューア不作動設定回数（Ｎ）」を設定テーブル１１から読み出してＤＢカードに書き込む（ステップＢ５）。

【００３６】

更に、現在のシステム日時を取得し、これを時間変数キーとして特定しておく（ステップＢ６）。そして、特定グループの各ユーザのうち、その先頭のユーザから対応する「パスワード」を読み出し（ステップＢ７）、上述の時間変数をキーとして、この「パスワード」を暗号化する（ステップＢ８）。これによって生成された暗号化パスワードに「時間変数キー」を付加して、対応するユーザ名と共にＤＢカードに書き込む（ステップＢ９）。

そして、特定グループの各ユーザを全て指定し終わったかを調べ（ステップＢ１０）、全て指定し終わるまでステップＢ７に戻り、上述の動作を各ユーザ毎に繰り返す。これによって全ユーザ分の処理が終了すると、設定テーブル１１から特定グループの「レコード暗号化キー（ＲＫ）」を読み出してＤＢカードに書き

込む（ステップＢ１１）。

【００３７】

次に、モバイルＤＢ作成してＤＢカードに書き込む処理に移る。

先ず、設定テーブル１１に登録されている特定グループ対応の各モバイルＤＢ名のうち、その先頭のモバイルＤＢ名に対応づけられているマスタＤＢ名に該当するマスタＤＢファイルを読み出しておく（ステップＢ１２）。そして、このマスタＤＢ名対応の「レコード抽出条件」、「抽出対象フィールド」をそれぞれ取得し、この「レコード抽出条件」に基づいてマスタＤＢファイル１２を検索することにより該当レコードを抽出する（ステップＢ１３）。すなわち、図１２（Ｂ）は、この場合の具体例を示し、マスタＤＢ（図１２（Ａ）参照）から「レコード抽出条件」に該当する各レコード群を切り出すことによって、当該グループの業務内容や端末の処理内容に必要なレコード群のみが抽出される。

【００３８】

これによって抽出した各レコード群を「抽出対象フィールド」に基づいて、そのレコード構成を変更する（ステップＢ１４）。図１３（Ｃ）は、この場合の具体例を示し、抽出されたレコード群は、それを構成する各フィールドのうち、「抽出対象フィールド」に該当するフィールドのみが切り出され、切り出されたフィールドのみからなるレコード構成に変更される。

次に、図１１のステップＢ１５に移り、上述のようにレコード構成を変更した後の各レコード・フィールドを「レコード暗号化キー（ＲＫ）」に基づいて暗号化する。この場合、各レコード・フィールドを暗号化する毎に、「レコード暗号化キー（ＲＫ）」の値を更新することによって、それぞれ異なるキーを用いて個別に暗号化するようにしている。そして、暗号化したレコード群をモバイルＤＢファイルとして作成して、ＤＢカードに書き込む（ステップＢ１６）。

このようにして１ファイル分のモバイルＤＢを作成すると、特定グループに対応して他のモバイルＤＢ名が設定登録されているかを調べ（ステップＢ１７）、有れば、ステップＢ１２に戻り、上述の動作を繰り返す。

これによって、特定グループ対応の各モバイルＤＢ名毎に、モバイルＤＢファイルが作成されてＤＢカード内に書き込まれると共に、そのファイルの格納位置

を示すＦＡＴが作成されてＤＢカード内に書き込まれる。

【００３９】

次に、モバイルＤＢ対応のカスタマイズＡＰをＤＢカードに書き込む処理に移る。先ず、マスタＤＢ名に基づいてそれに対応付けられているカスタマイズＡＰを設定テーブル１１から読み出し（ステップＢ１８）、それに対応カスタマイズＡＰがＤＢカード内に存在しているかを調べるが（ステップＢ２０）、最初は存在していないので、ステップＢ２４に進み、設定テーブル１１内の現行のカスタマイズＡＰを読み出してＤＢカードに上書きする。これによってＤＢカード内には、モバイルＤＢに対応して最新のカスタマイズＡＰ（「ソフト識別番号」、「更新日付」を含む）が新規に書き込まれる

【００４０】

また、ＤＢカード内にカスタマイズＡＰは存在している場合であっても（ステップＢ１９）、そのＤＢカード内の「更新日付」と、現行のカスタマイズＡＰの「更新日付」とを比較し、両者の不一致が判別された場合（ステップＢ２０）、つまり、現行のカスタマイズＡＰが更新されている場合にも、ステップＢ２４に進み、現行のカスタマイズＡＰをＤＢカードに上書きすることによって最新のカスタマイズＡＰに書き換えられる。なお、「更新日付」が一致する場合には、ＤＢカード内のカスタマイズＡＰは最新のものであるため、その更新は行われない。

そして、同一グループ内に他のカスタマイズＡＰが設定されているかを調べ（ステップＢ２１）、有れば、ステップＢ１８に戻り、次のカスタマイズＡＰを読み出し、以下同様の処理を繰り返す。

そして、カスタマイズＡＰの書き込みが終わると、ＤＢカード内のモバイルＤＢの各ファイル格納位置を示すＦＡＴを「スクランブルキー（ＳＫ）」を用いてスクランブル化する（ステップＢ２２）。

【００４１】

これによってＤＢカード１枚分の書き込み処理が終わると、未書き込みのＤＢカードが他に有るかを判別し（ステップＢ２３）、他のＤＢカードがセットされていれば、図１０のステップＢ２に戻り、未書き込みのＤＢカードの中からその

１つを指定して上述の動作を繰り返す。これによってサーバ装置にセットされている各ＤＢカードには、図６に示した内容がそれぞれ書き込まれる。

このようにして基本ソフト、ユーザ情報、モバイルＤＢ、対応カスタマイズＡＰ等が書き込まれたＤＢカードは、グループ毎に当該ユーザに配布される。

【００４２】

図１３は、携帯端末装置側において電源投入に応じて実行開始されるフローチャートである。

先ず、携帯端末装置にＤＢカードがセットされている状態において、電源がオンされると、ＤＢカード内の基本ソフトに基づいて基本動作が開始される（ステップＣ１）。すると、上述した第１セキュリティ層のＤＢカードセキュリティ処理が実行される。すなわち、ＤＢカードから「ハード識別番号」を読み出し（ステップＣ２）、当該端末内の「ハード識別番号」と照合する（ステップＣ３）。この結果、両者が一致する場合には（ステップＣ４）、当該端末とカードとは正当な対応関係にあるので、ＤＢカード内のスクランブル済み「ＦＡＴ」を端末側に読み込み、これを図６で示したＲＡＭ内の「ＦＡＴ読み出しエリア」にセットし（ステップＣ５）、この「ＦＡＴ」を端末内の「スクランブルキー（ＳＫ）」を用いてそのスクランブルを解除する（ステップＣ６）。そして、検索ビューアを起動させる（ステップＣ７）。

また、当該端末とカードとが正当な対応関係にない場合には、「ハード識別番号」の不一致が判別されるので、ハードエラー表示を行った後（ステップＣ８）、電源を強制的にオフし（ステップＣ９）、エラー終了となる。

【００４３】

図１４は、図１３のステップＣ７（検索ビューア起動）時の動作を詳述するためのフローチャートである。

先ず、上述した第２セキュリティ層のパスワード認証処理において、その前段階としてのセキュリティ処理が実行される。すなわち、携帯端末装置は検索ビューア起動時にＤＢカードをアクセスし、カード内に「動作制御管理ファイル」が存在しているかをチェックする（ステップＤ１）。ここで、上述したように、パスワードの誤入力が連続して何回か繰り返された場合、それ以降、検索ビュー

アを不作動とするために、「動作制御管理ファイル」を削除するようにしている。したがって、「動作制御管理ファイル」の存在有無をチェックし、それが存在していなければ、不作動メッセージを表示させた後（ステップＤ１１）、電源を強制的にオフして（ステップＤ１１）、エラー終了となる。

【００４４】

一方、「動作制御管理ファイル」が存在していれば、それを条件としてログイン入力画面を表示させてユーザ名、パスワード入力を促すメッセージを表示する（ステップＤ２）。ここで、オペレータが自己の「ユーザ名」、「パスワード」を入力すると（ステップＤ３）、ＤＢカード内の「ユーザ名」対応の暗号化パスワードを読み出し（ステップ）、この暗号化パスワードを「時間変数」をキーとして復号化する（ステップＤ５）。そして、入力されたパスワードと復号化されたパスワードとを照合する（ステップＤ６）。

その結果、両者の不一致が判別された場合には（ステップＤ７）、その不一致回数を更新すると共に、その更新値と、予めグループ毎に設定されている「ビューア不作動設定回数（Ｎ）」とを比較し、パスワードの誤入力が連続してＮ回繰り返されたかをチェックし（ステップＤ８）、Ｎ回未満であれば、ログイン入力画面に戻り（ステップＤ２）、その再入力を受け付ける。

いま、パスワードの誤入力が連続してＮ回繰り返されたことが判別された場合には（ステップＤ８）、「動作制御管理ファイル」を削除すると共に（ステップＤ９）、不作動メッセージを表示させた後（ステップＤ１０）、電源を強制的にオフして（ステップＤ１１）、エラー終了となる。

【００４５】

また、パスワードの誤入力が連続してＮ回繰り返される前において、パスワードが一致し、正当のオペレータであることが判別された場合には（ステップＤ７）、先ず、上述した第３セキュリティ層のソフトセキュリティ処理が行われる。すなわち、ＤＢカード内に書き込まれている各カスタマイズＡＰのメニュ画面が一覧表示されるので、このメニュ画面の中からオペレータが所望するカスタマイズＡＰを選択指定すると（ステップＤ１２）、選択されたカスタマイズＡＰに含まれている「ソフト識別番号」をＤＢカード内から読み出し（ステップＤ１３）

、自己の端末内の「ソフト識別番号」と照合する（ステップＤ１４）。その結果、両者の不一致が判別された場合には（ステップＤ１５）、不作動メッセージ表示を行うと共に（ステップＤ１０）、電源を強制的にオフして（ステップＤ１１）、エラー終了となる。

一方、「ソフト識別番号」を照合した結果、両者の一致が判別された場合には、選択されたカスタマイズＡＰを立ち上げ、それに応じたアプリケーション処理を実行開始させる（ステップＤ１６）。

【００４６】

図１５および図１６は、図１４のステップＤ１６（カスタマイズＡＰ起動）時の動作を詳述するためのフローチャートである。

先ず、処理メニュ表示が行われる（ステップＥ１）。この場合のメニュ画面には「キー検索」、「追加」、「終了」の各メニュ項目が表示され、その中から所望するメニュ項目を選択指定すると（ステップＥ２）、選択項目を調べ（ステップＥ３、Ｅ１３）それにに応じた処理に移る。

【００４７】

ここで、メニュ項目「キー検索」が選択された場合において、検索キー（例えば、商品名や得意先名等）が入力されると（ステップＥ４）、ＤＢカードから「レコード暗号化キー」を読み込み、この検索キーを「レコード暗号化キー（ＲＫ）」で暗号化する（ステップＥ５）。そして、ＤＢカード内のモバイルＤＢを暗号化された検索キーを用いて検索して（ステップＥ６）、そのキーに該当するレコードを抽出するが、一致するキーが無ければ（ステップＥ７）、メニュ表示画面に戻り（ステップＥ１）、検索キーの再入力が可能となる。

いま、キー検索の結果、一致するキーが有れば（ステップＥ７）、ステップＥ８に移り、当該モバイルＤＢから検索キーに該当するレコードを読み出して、図６で示したＲＡＭ内の「レコードエリア」に書き込む。そして、このレコードを「レコード暗号化キー（ＲＫ）」で復号化して（ステップＥ９）、そのレコード内容を表示出力させると共に（ステップＥ１０）、処理メニュ表示が行われる（ステップＥ１１）。

【００４８】

この場合のメニュ画面には「訂正」、「削除」、「終了」の各メニュ項目が表示されるので、その中から所望するメニュ項目を選択指定する（ステップＥ１２）。すると、選択項目を調べ（図１６のステップＥ２０、Ｅ２６）それにに応じた処理に移る。

すなわち、メニュ項目「訂正」が選択された場合において（ステップＥ２０）、訂正データが入力されると、それに応じてレコード内容を訂正する処理が行われる（ステップＥ２１）。そして、レコード訂正が行われたことを示すために、その訂正レコードに「訂正フラグ」をセットすると共に（ステップＥ２２）、訂正レコードを「レコード暗号化キー（ＲＫ）」を用いて暗号化し（ステップＥ２３）、この暗号化レコードを当該モバイルＤＢ内の元のレコードに上書きする（ステップＥ２４）。

これによってレコード訂正が終了すると、その端末内から当該レコードを削除しておく（ステップＥ２５）。つまり、図６で示したＲＡＭ内の「レコードエリア」をクリアする。

また、メニュ項目「削除」が選択された場合には（ステップＥ２６）、該当レコードのデータ部を削除し、そのレコードに「削除フラグ」をセットして、当該モバイルＤＢ内の元のレコードに上書きする（ステップＥ２７）。そして、端末内から当該レコードを削除しておく（ステップＥ２５）。

【００４９】

他方、図１５のステップＥ１での処理メニュ画面において、「追加」が選択された場合には、ステップＥ１４に移り、新規レコードの入力作成処理が行われる。そして、レコード追加であることを示すために、新規レコードに「追加フラグ」をセットすると共に（ステップＥ１５）、新規レコードを「レコード暗号化キー（ＲＫ）」を用いて暗号化し（ステップＥ１６）、この暗号化レコードを当該モバイルＤＢ内に追加する（ステップＥ１７）。

これによってレコード追加が終了すると、その端末内から当該レコードを削除しておく（図１６のステップＥ２５）。

なお、図１６のステップＥ１での処理メニュ画面において、「終了」が選択された場合には、端末内の「ＦＡＴ」を削除する（ステップＥ１８）。つまり、図

６で示したＲＡＭ内の「ＦＡＴ読み出しエリア」の内容をクリアする。そして、その端末内のレコードを削除する（ステップＥ２５）。

このようにして、携帯端末装置側では、ＤＢカードに格納されているモバイルＤＢのファイル内容が日常業務の遂行に応じて更新される。

【００５０】

図１７は、サーバ装置において、日常業務の遂行に応じて変更されたＤＢカード内のモバイルＤＢを収集してサーバ内のマスタＤＢを更新する場合の動作（回収動作）を示したフローチャートである。

先ず、オペレータが回収対象のＤＢカードをサーバ装置にセットすると（ステップＦ１）、このＤＢカードから「ハード識別番号」を読み出し（ステップＦ２）、この「ハード識別番号」に基づいて設定テーブル１１を参照し、それに該当するグループを特定する（ステップＦ３）。そして、ＤＢカードから「スクランブルキー（ＳＫ）」を読み出し、ＤＢカード内のＦＡＴを「スクランブルキー（ＳＫ）」を用いてスクランブル解除する（ステップＦ４）。

また、ＤＢカードからモバイルＤＢを読み出し（ステップＦ５）、このＤＢファイルの各レコード・フィールドを「レコード暗号化キー（ＲＫ）」を用いて復号化する（ステップＦ６）。この場合においても、各レコード・フィールドを復号化する毎に、「レコード暗号化キー（ＲＫ）」の値を更新することによって、それぞれ異なるキーを用いて復号化を行うようにしている。

【００５１】

そして、復号化したＤＢファイル内に変更レコードが存在するかを「訂正フラグ」、「削除フラグ」、「追加フラグ」の有無に基づいて調べ（ステップＦ７）、変更レコードが有れば、つまり、いずれかの「フラグ」が付加されているレコードが存在していれば、そのモバイルＤＢに対応するサーバ装置内のマスタＤＢを特定し（ステップＦ８）、当該モバイルＤＢから読み出した変更レコードをそれに付加されている「フラグ」の種類に応じてマスタＤＢ内の該当レコードを更新する処理を行う（ステップＦ９、Ｆ１０）。

すなわち、該当するレコード内容を訂正する訂正処理、該当レコードのデータ部を削除する削除処理、新規レコードを追加する追加処理を行う。このようなマ

スタＤＢのレコード更新処理は、モバイルＤＢ内の全ての変更レコードに対して行われる（ステップＦ９～Ｆ１１）。そして、他のモバイルＤＢがＤＢカード内に有れば（ステップＦ１２）、そのモバイルＤＢに対して上述の動作を繰り返す（ステップＦ５～Ｆ１２）。

【００５２】

以上のように、この一実施形態おいては、携帯端末装置がＤＢカードをアクセスする際、このカード内の「ハード識別番号」と自己の「ハード識別番号」とを照合し、その照合結果に基づいて当該ＤＢカードに対するアクセス可否を決定し、その結果、当該カードに対するアクセスが許可された際に、このカードに記憶されている「ソフト識別番号」と自己の「ソフト識別番号」とを照合し、その照合結果に基づいて当該カード内のモバイルＤＢへのアクセス可否を決定するようにしたから、端末と媒体との対応付けにより、そのモバイルＤＢに対するアクセスの他、このカード自体に対するアクセスをも不可能とする多重セキュリティという万全な対策を講じることができる。

【００５３】

これによって、紛失、盗難、悪意等によってＤＢカード内のモバイルＤＢが他人に漏洩されることを確実に防止することができる。また、セキュリティ管理のために特別な操作を要求せず、操作性を損なわないセキュリティ管理を実現することができる。すなわち、ＤＢカードを携帯端末装置に装着するだけで自動的にセキュリティ管理が実行されるので、ＤＢカード利用時にユーザはセキュリティ対策を全く意識しなくてもよく、使い勝手を損なわず、確実なセキュリティ管理を実現することができる。

この場合、重要情報を含んだモバイルＤＢを携帯端末から分離可能なＤＢカードだけに保管しておくようにしたから、携帯端末のみを紛失したり、盗難されたとしてもセキュリティ上全く問題は無く、また、ＤＢカードを紛失したり、盗難された場合でも、そのカードへのアクセスは、正当の端末しかできないようにした仕組みを持っているため、モバイルＤＢに対するアクセスはおろか、ＤＢカード自体に対するアクセスをも不可能となり、そのセキュリティは極めて高いものとなる。

【００５４】

また、サーバ装置は、ＤＢカードに配布すべきモバイルＤＢの各レコードを個別に暗号化して当該ＤＢカードに書き込み、携帯端末装置は、それにセットされているＤＢカードが当該端末に対応付けられている正当な媒体かを判別し、端末対応の媒体であれば、そのＤＢカード内のモバイルＤＢへのアクセスを許可すると共に、アクセス対象として任意に指定されたレコードを個別に読み込み、この１レコード分のデータを復号化してそのレコード内容を表示するようにしたから、当該カードをアクセスする場合でも、暗号化されたままの状態で行うことができ、カードの紛失、盗難あるいは悪意等において、仮に、正当な端末以外がモバイルＤＢのアクセスまでたどり着いた最悪のケースでも、復号化されたレコードのみのセキュリティが問題になるだけで、そのモバイルＤＢの全貌が解読される危険性はなく、重要情報の漏洩を確実に防止することが可能となる。

【００５５】

ここで、携帯端末装置は、モバイルＤＢに対するアクセス終了時あるいはその端末処理終了時において、ＲＡＭ内の「レコードエリア」に一時記憶されている復号化されたままの状態にあるレコード内容を消去するようにしたから、端末内にはその処理残片もなくなり、更に効果的なセキュリティ管理が可能となる。

また、ＤＢカード内のモバイルＤＢは各レコード・フィールド毎に個別に暗号化されており、携帯端末装置はアクセス対象として任意に入力された検索キーを暗号化すると共に、暗号化された検索キーに基づいてモバイルＤＢを検索することにより、検索キーに該当するフィールドを持つレコードを個別に読み込み、この読み込んだレコードを復号化して表示するようにしたから、モバイルＤＢを各レコード・フィールド毎に暗号化したとしても、所望するフィールドをキーとしてモバイルＤＢの検索が可能となる。

また、ＤＢカード内のモバイルＤＢから個別に読み込んでそれを復号化したレコードに対してその変更が指示されたり、当該モバイルＤＢに対して新規レコードの追加が指示された場合において、その変更されたレコードや追加されたレコードを暗号化すると共に、暗号化されたレコードをモバイルＤＢに対する更新情報としてＤＢカード内に書き込むようにしたから、端末側で変更・追加されたレ

コードの暗号化により、更に効果的なセキュリティ管理が可能となる。

【００５６】

また、サーバ装置は、ＤＢカードへのモバイルＤＢ等を書き込む際に、ＤＢカードとそれをアクセス可能な携帯端末装置との対応付けと、ＤＢカードとそれを利用可能なユーザとの対応付けを一括して行うようにしたから、その設定作業を効率よく行うことができると共に、ＤＢカードに対するセキュリティ管理を確実なものとするために、その対策を講じるための仕組みを携帯端末装置自体に持たせず、また、セキュリティ管理のためにユーザに特別な操作を要求せず、操作性を損なわない確実なセキュリティ管理を実現することができる。

【００５７】

なお、「ハード識別番号」、「ソフト識別番号」をどのような情報に基づいて生成するかは任意であり、例えば、「ハード識別番号」をその携帯端末装置の「製造会社コード」＋「製造番号」等で構成してもよい。また、同一ＤＢカード内に複数のモバイルＤＢが格納されている場合に、各モバイルＤＢ毎に「ソフト識別番号」を相違させてもよい。

また、端末グループは、複数の端末を単に区分けする以外に、1台の端末が複数のグループに属するような設定も可能である。

また、モバイルＤＢファイルを作成する際に、「レコード暗号化キー（ＲＫ）」の値を更新することによって、それぞれ異なるキーを用いて各レコード・フィールドを個別に暗号化するようにしたが、「レコード暗号化キー（ＲＫ）」を各レコード毎に用意しておき、対応するキーを用いて各レコードを暗号化するようにしてもよい。また、「レコード暗号化キー（ＲＫ）」を携帯端末装置側に記憶管理させてもよい。

その他、モバイルＤＢファイルにおけるＦＡＴをスクランブル化した場合を示したが、モバイルＤＢファイル自体をスクランブル化するようにしてもよい。更に、パスワードにおいても、時間変数をキーとして暗号化する場合に限らないことは勿論である。

【００５８】

また、上述した一実施形態においては、可搬型記憶媒体であるＤＢカードとし

て、コンパクトフラッシュカードを例示したが、その他にＰＣカード、スマートメディア、ＣＤ（光ディスク）、ＭＯ（光磁気ディスク）、ＦＤ（フロッピーディスク）等であってもよく、しかも、カード型に限らず、カセット型、スティック型等、その形状は任意である。

更に、携帯端末装置としては、電子手帳、ノート型パソコン、ＰＤＡ、携帯電話等であってもよい。

【００５９】

【発明の効果】

この発明によれば、可搬型データ記憶媒体内のデータファイルを各レコード毎に暗号化しておくことで、当該記憶媒体をアクセスする場合でも、暗号化されたままの状態で行うことができ、記憶媒体の紛失、盗難あるいは悪意等において、仮に、正当な端末以外がデータファイルのアクセスまでたどり着いた最悪のケースでも、復号化されたレコードのみのセキュリティが問題になるだけで、そのファイルの全貌が解読される危険性はなく、重要情報の漏洩を確実に防止することができる。

【図面の簡単な説明】

【図１】

セキュリティ管理システムの全体構成を示したブロック図。

【図２】

端末グループ対応のＤＢカード３を説明すると共に、携帯端末装置とユーザとの対応関係を説明するための図。

【図３】

多重セキュリティを概念的に示した図。

【図４】

（Ａ）は、サーバ装置側に設けられている設定テーブル１１の構成とその設定内容を示した図、（Ｂ）はマスタＤＢファイル１２を示した図、（Ｃ）はＤＢ対応基本ＡＰ１３を示した図。

【図５】

各ＤＢカード３に書き込まれた内容を示した図。

【図６】

各携帯端末装置２の内蔵メモリに書き込まれた内容を示した図。

【図７】

サーバ装置１、携帯端末装置２の全体構成を示したブロック図。

【図８】

サーバ装置１が設定テーブル１１に対して設定を行う場合の動作を示したフローチャート。

【図９】

図８に続く設定動作を示したフローチャート。

【図１０】

サーバ装置１がマスタＤＢやカスタマイズＡＰ等をＤＢカード３に書き込んで配布する場合の動作を示したフローチャート。

【図11】

図１０に続く配布動作を示したフローチャート。

【図12】

（Ａ）はマスタＤＢを示した図、（Ｂ）はマスタＤＢから「レコード抽出条件」によって抽出されたレコードを示した図、（Ｃ）は各抽出レコードから「抽出対象フィールド」によって変更された変更後のレコード構成を示した図。

【図13】

携帯端末装置２側において電源投入に応じて実行開始されるフローチャート。

【図14】

図１３のステップＣ７（検索ビューア起動）時の動作を詳述するためのフローチャート。

【図15】

図１４のステップＤ１６（ＤＢ対応のカスタマイズＡＰ起動）時の動作を詳述するためのフローチャート。

【図16】

図１５に続くカスタマイズＡＰ起動時の動作を詳述したフローチャート。

【図17】

サーバ装置１において、日常業務の遂行に応じて変更されたＤＢカード内のモバイルＤＢを収集してサーバ内のマスタＤＢを更新する場合の回収動作を示したフローチャート。

【符号の説明】

１　サーバ装置

２　携帯端末装置

３　ＤＢカード

１１　設定テーブル

１２　マスタＤＢファイル

１３　ＤＢ対応基本ＡＰ

２１、２１Ａ　ＣＰＵ

２２、２２Ａ　記憶装置

２３、２３Ａ　記録媒体

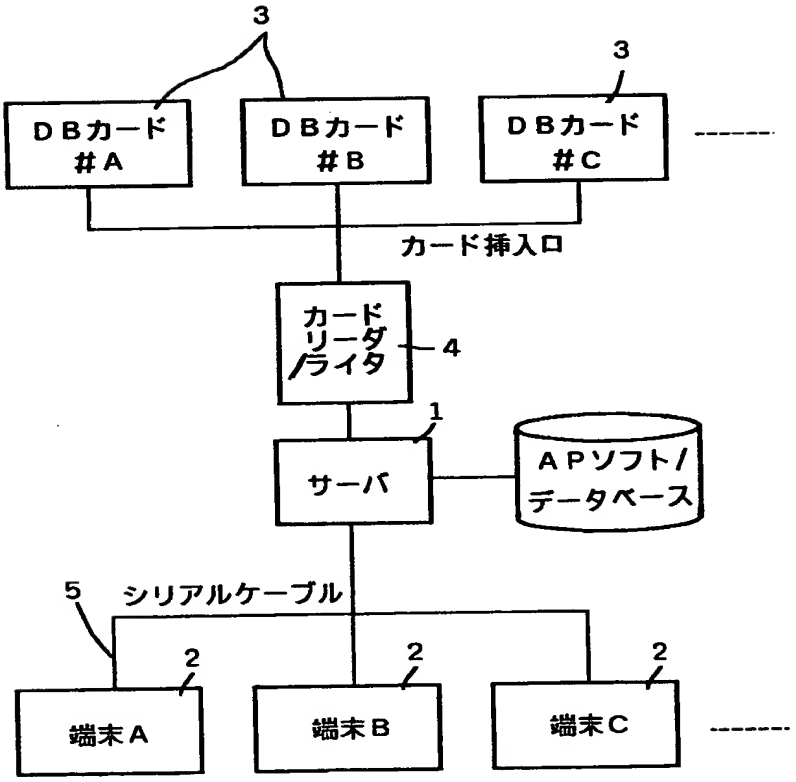
２５、２５Ａ　伝送制御部

２６、２６Ａ　入力部

２７、２７Ａ　表示部

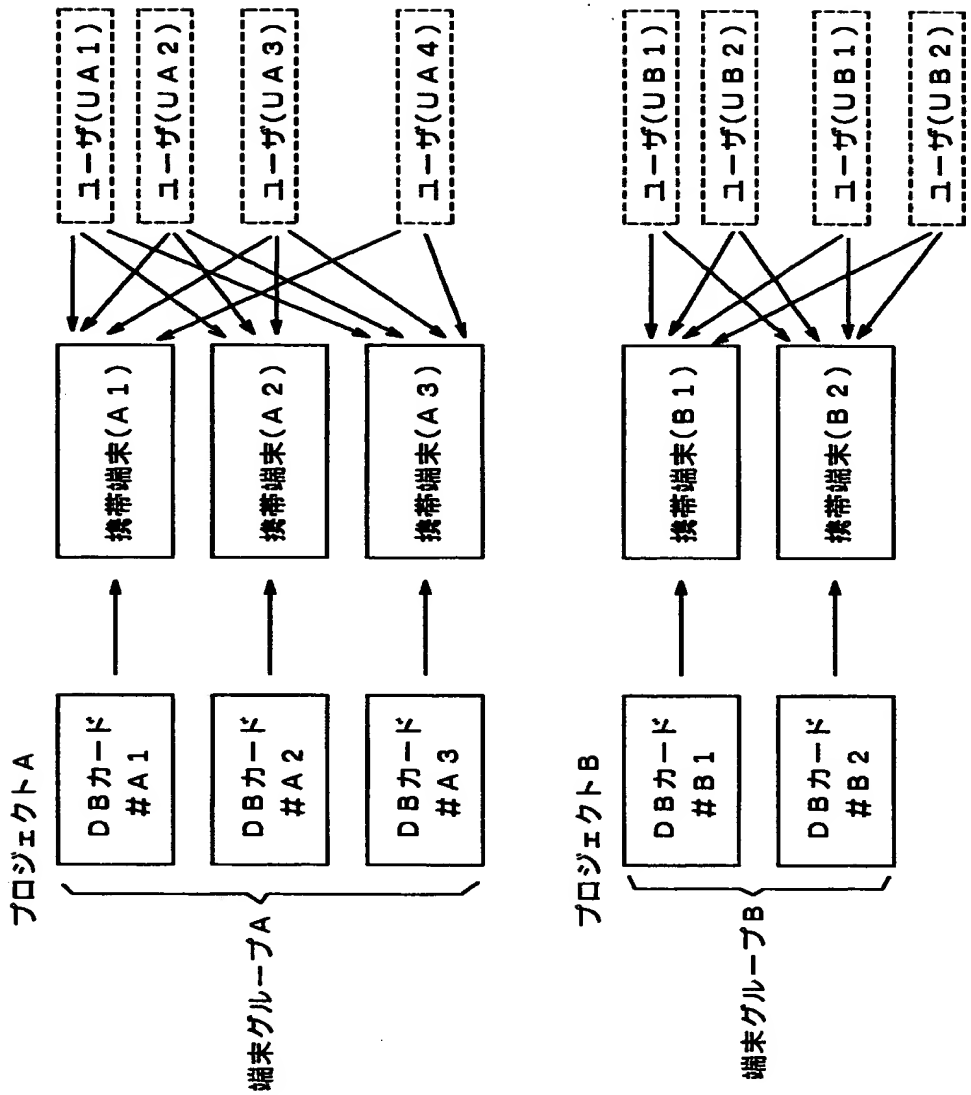
【書類名】　　図面

【図１】


3
3
3
ＤＢカード
＃Ａ
ＤＢカード
＃Ｂ
ＤＢカード
＃Ｃ

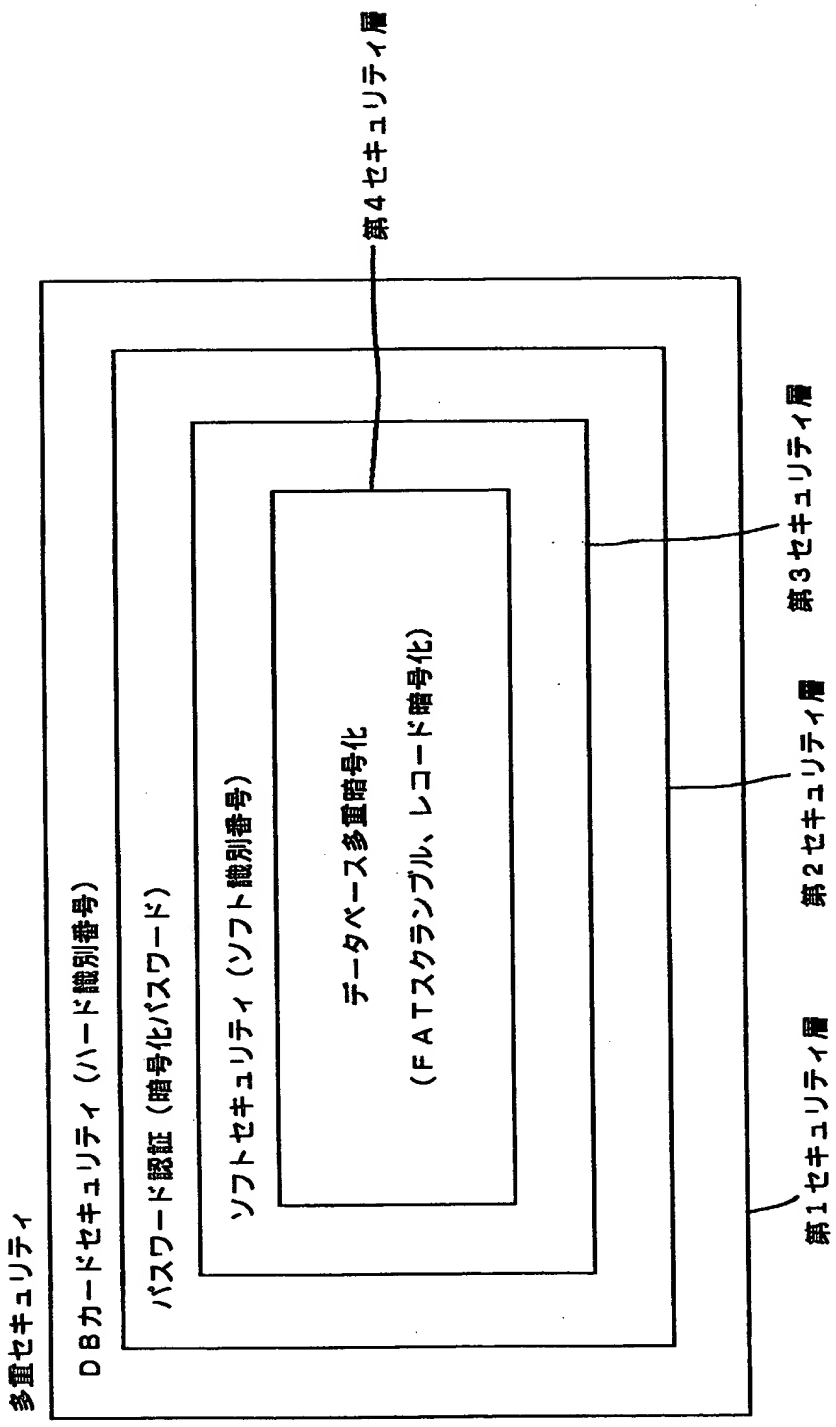
カード挿入口
カード
リーダ
/ライタ
4
1
サーバ
ＡＰソフト/
データベース
5
シリアルケーブル
2
2
2
端末Ａ
端末Ｂ
端末Ｃ

【図２】

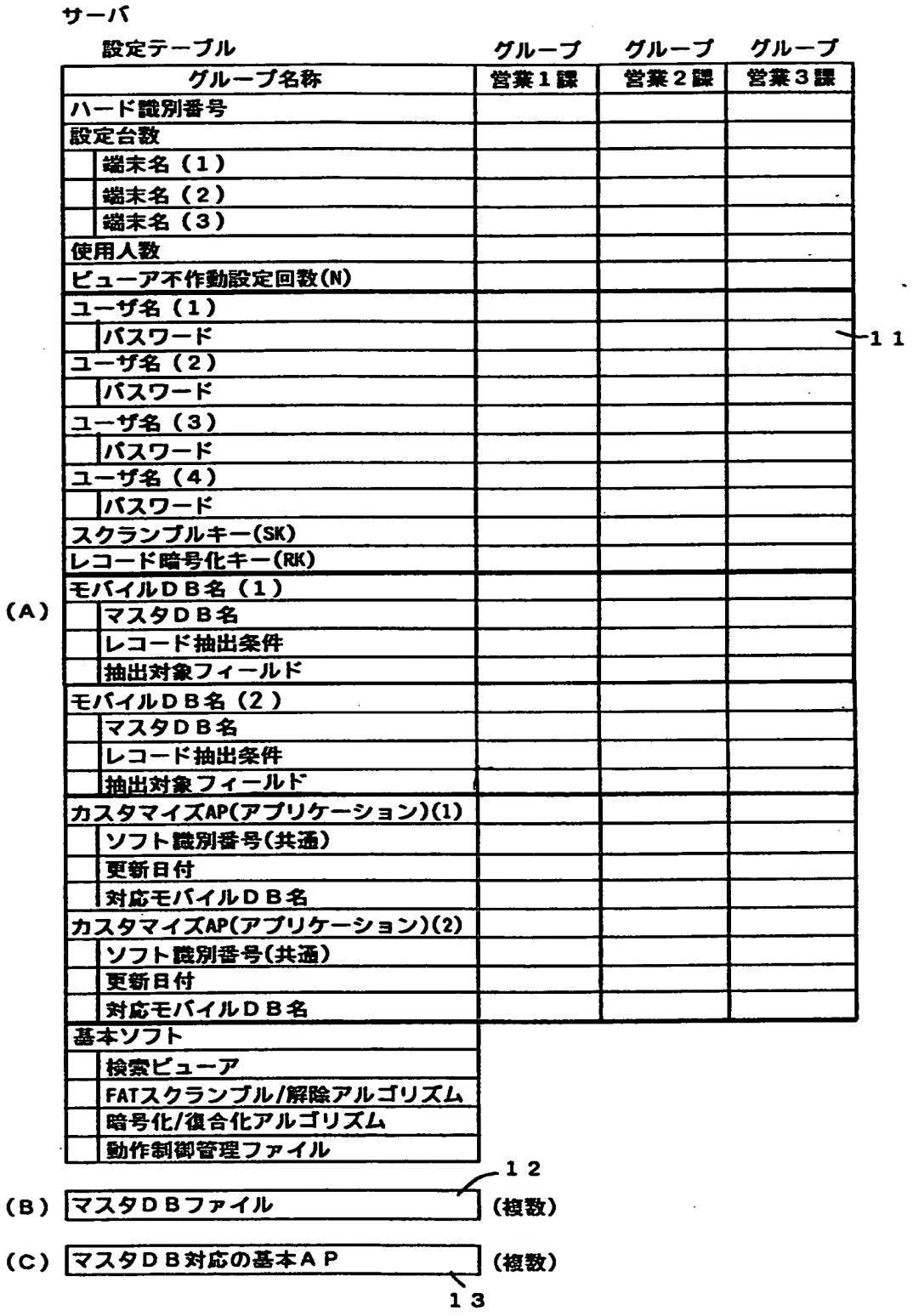


出証特２０００－３０２４１７９

【図３】


多重セキュリティ
ＤＢカードセキュリティ（ハード識別番号）
パスワード認証（暗号化パスワード）
ソフトセキュリティ（ソフト識別番号）
データベース多重暗号化
（ＦＡＴスクランブル、レコード暗号化）
第４セキュリティ層
第３セキュリティ層
第２セキュリティ層
第１セキュリティ層

【図４】


サーバ
設定テーブル
グループ
グループ
グループ
グループ名称
営業１課
営業２課
営業３課
ハード識別番号
設定台数
端末名（１）
端末名（２）
端末名（３）
使用人数
ビューア不作動設定回数(N)
ユーザ名（１）
パスワード
ユーザ名（２）
パスワード
ユーザ名（３）
パスワード
ユーザ名（４）
パスワード
スクランブルキー(SK)
レコード暗号化キー(RK)
モバイルＤＢ名（１）
(A)
マスタＤＢ名
レコード抽出条件
抽出対象フィールド
モバイルＤＢ名（２）
マスタＤＢ名
レコード抽出条件
抽出対象フィールド
カスタマイズAP(アプリケーション)(1)
ソフト識別番号(共通)
更新日付
対応モバイルＤＢ名
カスタマイズAP(アプリケーション)(2)
ソフト識別番号(共通)
更新日付
対応モバイルＤＢ名
基本ソフト
検索ビューア
FATスクランブル/解除アルゴリズム
暗号化/復合化アルゴリズム
動作制御管理ファイル
11
12
(B)
マスタＤＢファイル
(複数)
(C)
マスタＤＢ対応の基本ＡＰ
(複数)
13

【図５】

カード内部構成

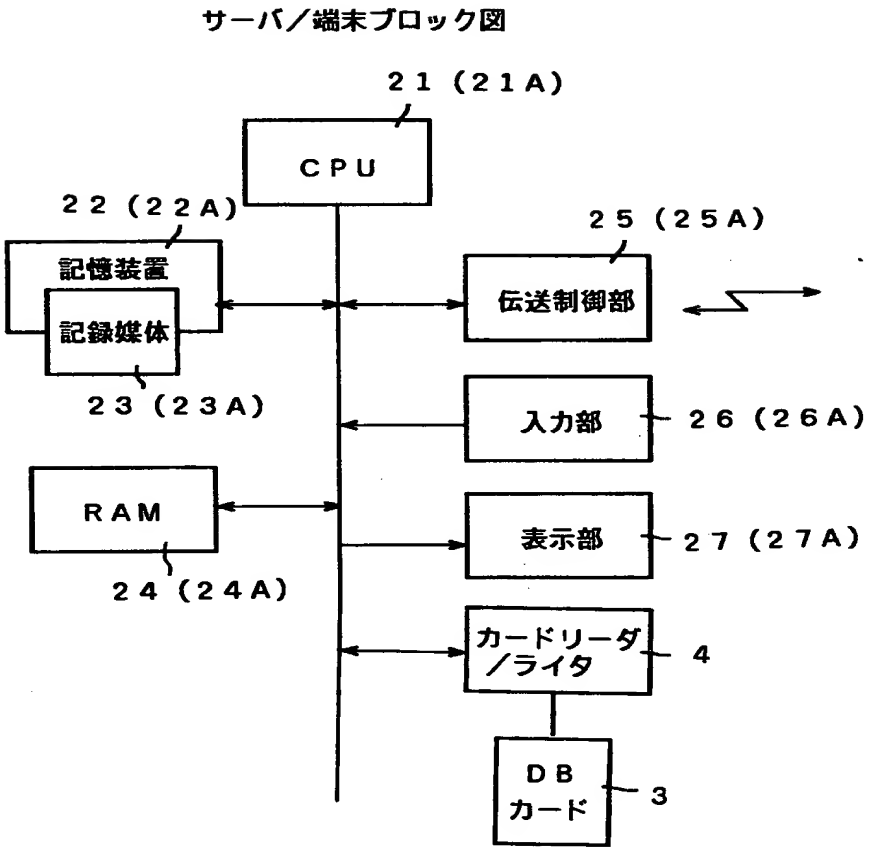
ハード識別番号（固定）
ＦＡＴ（スクランブル済）
基本ソフト
検索ビューア
ＦＡＴスクランブル／解除アルゴリズム
暗号化／復合化アルゴリズム
動作制御管理ファイル
ビユーア不作動設定回数（Ｎ）
ユーザ名（１）
暗号化パスワード＋時間変数キー
ユーザ名（２）
暗号化パスワード＋時間変数キー
ユーザ名（３）
暗号化パスワード＋時間変数キー
ユーザ名（４）
暗号化パスワード＋時間変数キー
レコード暗号化キー（ＲＫ）
モバイルＤＢ名（１）
ＤＢ（暗号済）
モバイルＤＢ名（１）
ＤＢ（暗号済）
カスタマイズＡＰ（１）
ソフト識別番号(共通)
更新日付
対応モバイルＤＢ名
カスタマイズＡＰ（２）
ソフト識別番号(共通)
更新日付
対応モバイルＤＢ名

【図６】

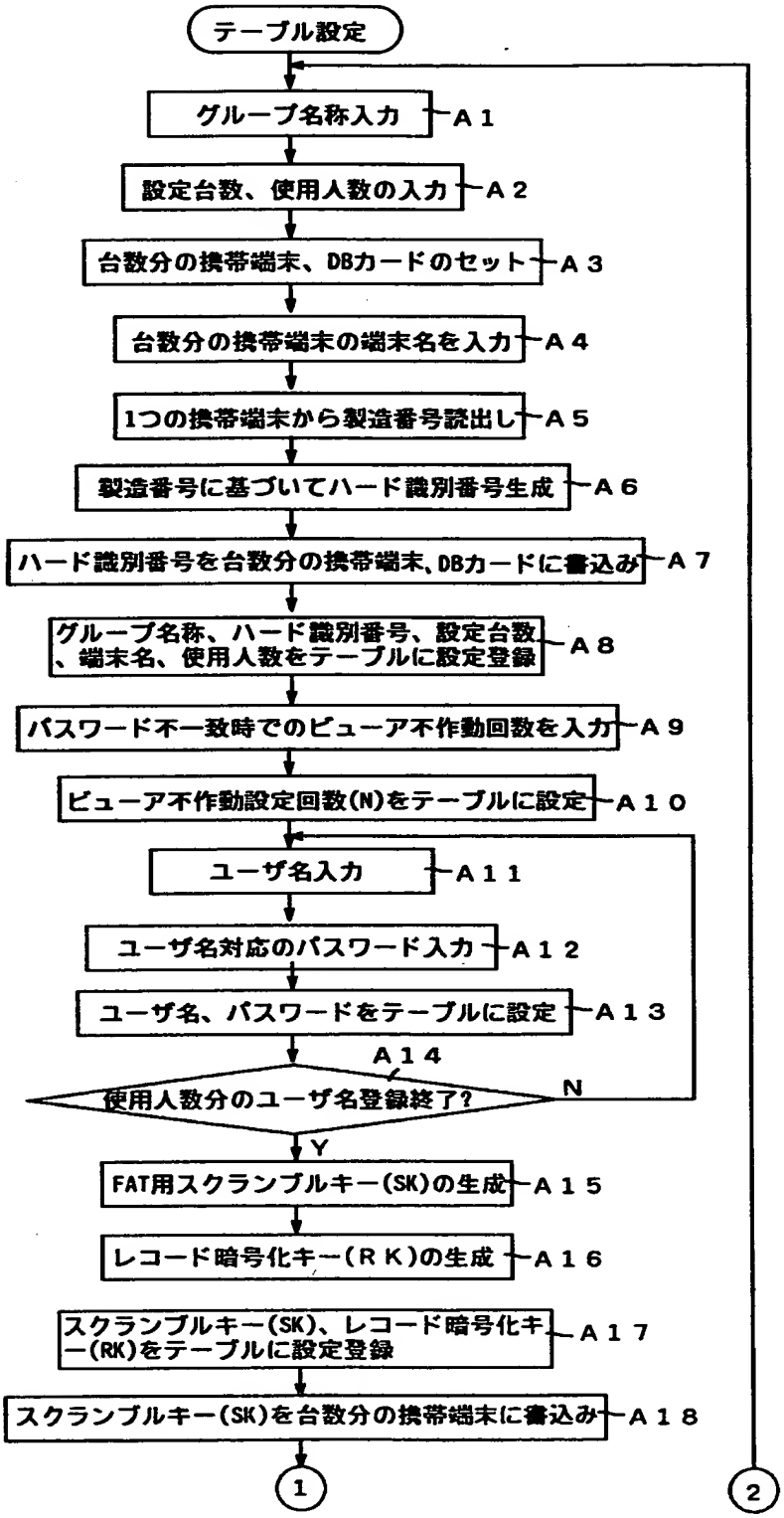
内蔵メモリ構成

ＦｌａｓｈＲＯＭ	
	ハード識別番号
	ソフト識別番号
	スクランブルキー（ＳＫ）
ＲＡＭ（一次記憶メモリ）	
	キー／データ入力エリア
	ＦＡＴ読出しエリア
	レコードエリア
	その他

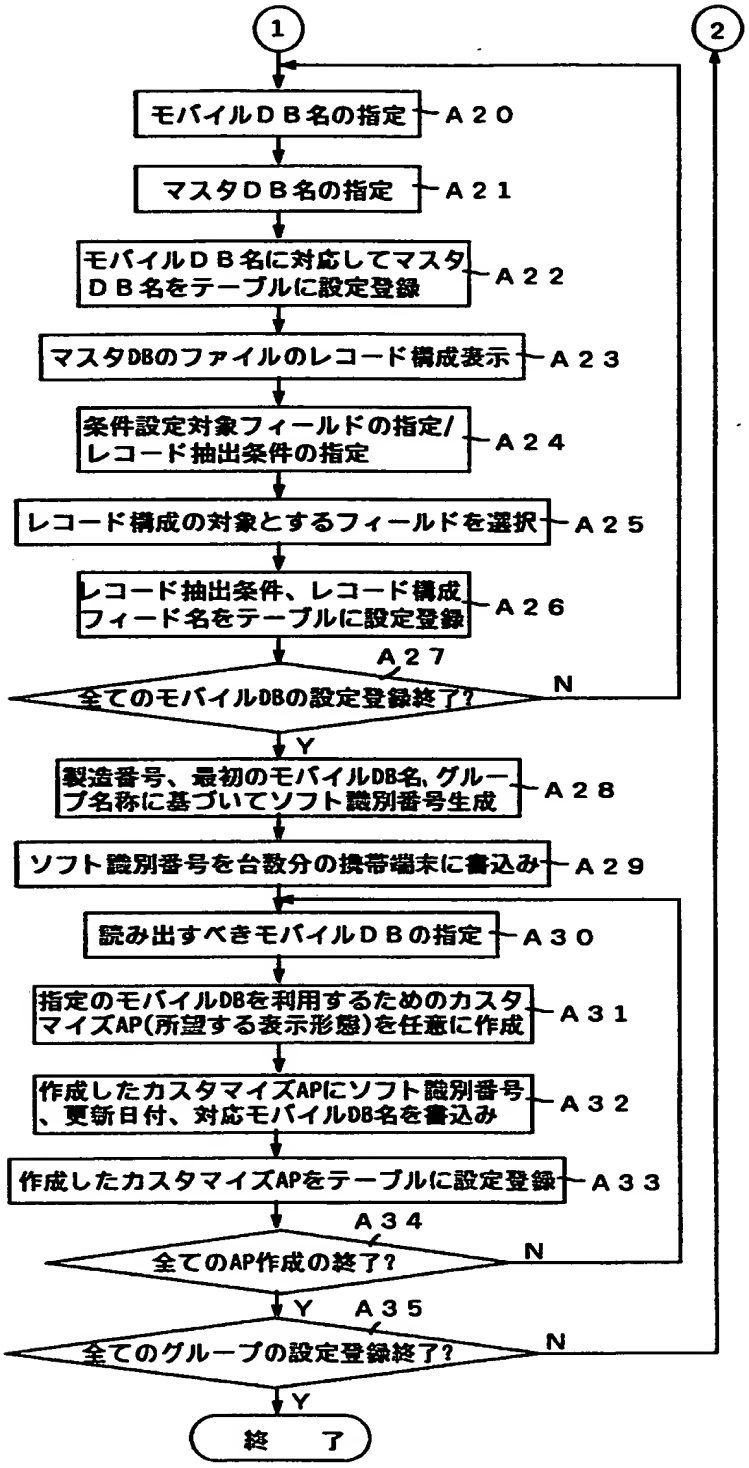
【図７】


サーバ／端末ブロック図
２１（２１Ａ）
ＣＰＵ
２２（２２Ａ）
記憶装置
記録媒体
２３（２３Ａ）
ＲＡＭ
２４（２４Ａ）
２５（２５Ａ）
伝送制御部
入力部
２６（２６Ａ）
表示部
２７（２７Ａ）
カードリーダ／ライタ
４
ＤＢカード
３

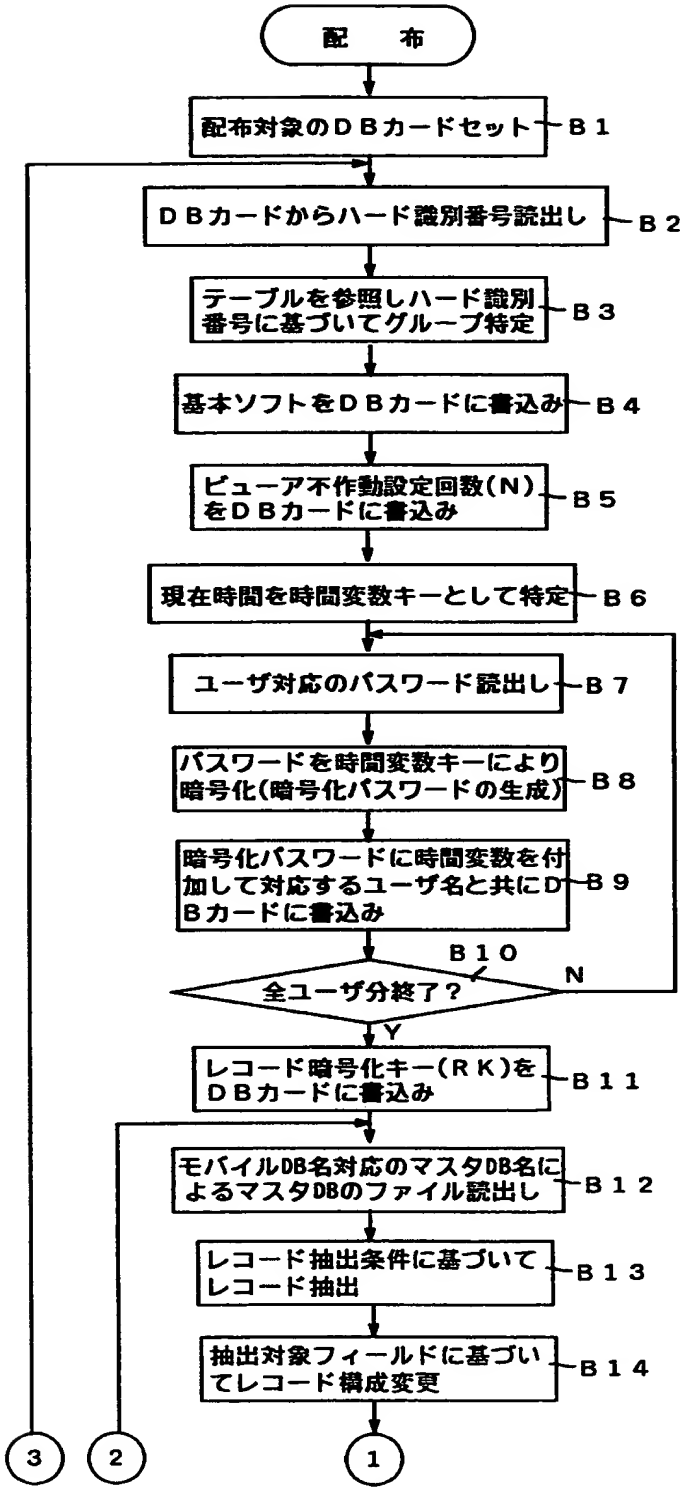
【図８】


テーブル設定
グループ名称入力
A１
設定台数、使用人数の入力
A２
台数分の携帯端末、DBカードのセット
A３
台数分の携帯端末の端末名を入力
A４
1つの携帯端末から製造番号読出し
A５
製造番号に基づいてハード識別番号生成
A６
ハード識別番号を台数分の携帯端末、DBカードに書込み
A７
グループ名称、ハード識別番号、設定台数、端末名、使用人数をテーブルに設定登録
A８
パスワード不一致時でのビューア不作動回数を入力
A９
ビューア不作動設定回数(N)をテーブルに設定
A１０
ユーザ名入力
A１１
ユーザ名対応のパスワード入力
A１２
ユーザ名、パスワードをテーブルに設定
A１３
A１４
使用人数分のユーザ名登録終了?
N
Y
FAT用スクランブルキー(SK)の生成
A１５
レコード暗号化キー(ＲＫ)の生成
A１６
スクランブルキー(SK)、レコード暗号化キー(RK)をテーブルに設定登録
A１７
スクランブルキー(SK)を台数分の携帯端末に書込み
A１８
1
2

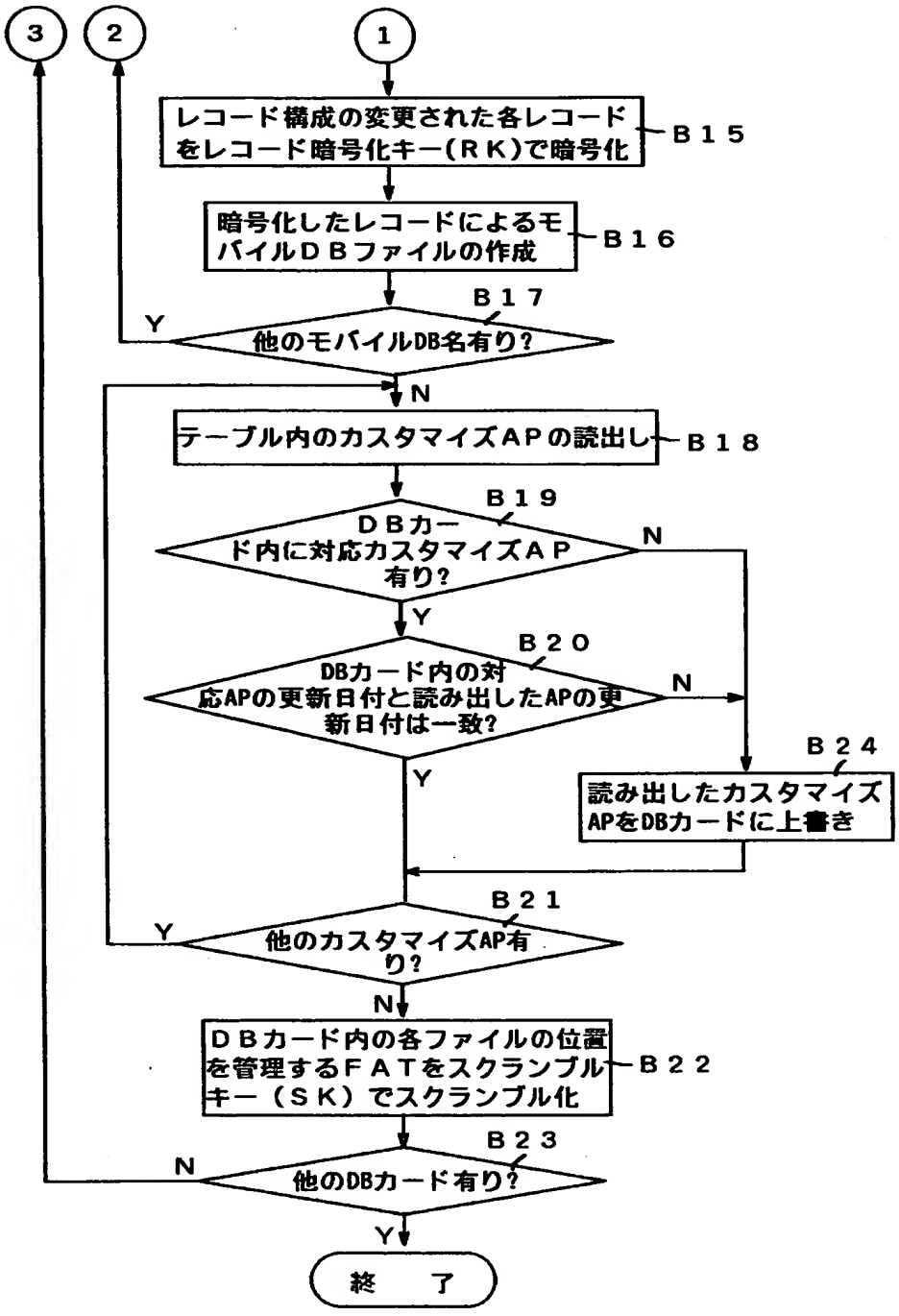
【図９】


1
2
モバイルＤＢ名の指定
Ａ２０
マスタＤＢ名の指定
Ａ２１
モバイルＤＢ名に対応してマスタＤＢ名をテーブルに設定登録
Ａ２２
マスタDBのファイルのレコード構成表示
Ａ２３
条件設定対象フィールドの指定/レコード抽出条件の指定
Ａ２４
レコード構成の対象とするフィールドを選択
Ａ２５
レコード抽出条件、レコード構成フィード名をテーブルに設定登録
Ａ２６
Ａ２７
全てのモバイルDBの設定登録終了?
N
Y
製造番号、最初のモバイルDB名、グループ名称に基づいてソフト識別番号生成
Ａ２８
ソフト識別番号を台数分の携帯端末に書込み
Ａ２９
読み出すべきモバイルＤＢの指定
Ａ３０
指定のモバイルDBを利用するためのカスタマイズAP(所望する表示形態)を任意に作成
Ａ３１
作成したカスタマイズAPにソフト識別番号、更新日付、対応モバイルDB名を書込み
Ａ３２
作成したカスタマイズAPをテーブルに設定登録
Ａ３３
Ａ３４
全てのAP作成の終了?
N
Y
Ａ３５
全てのグループの設定登録終了?
N
Y
終　了

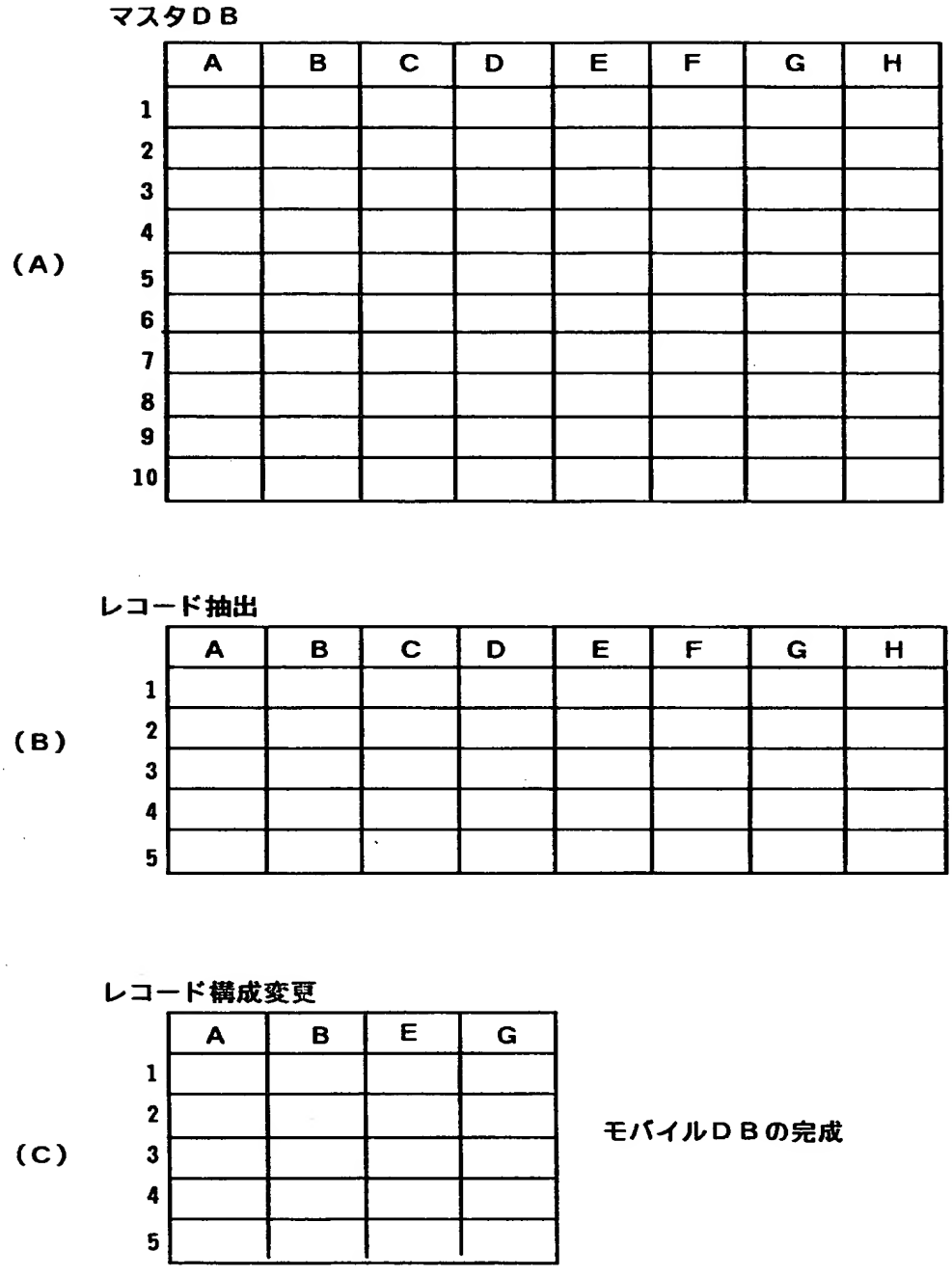
【図１０】


配　布
配布対象のＤＢカードセット
Ｂ１
ＤＢカードからハード識別番号読出し
Ｂ２
テーブルを参照しハード識別番号に基づいてグループ特定
Ｂ３
基本ソフトをＤＢカードに書込み
Ｂ４
ビューア不作動設定回数(Ｎ)をＤＢカードに書込み
Ｂ５
現在時間を時間変数キーとして特定
Ｂ６
ユーザ対応のパスワード読出し
Ｂ７
パスワードを時間変数キーにより暗号化(暗号化パスワードの生成)
Ｂ８
暗号化パスワードに時間変数を付加して対応するユーザ名と共にＤＢカードに書込み
Ｂ９
Ｂ１０
全ユーザ分終了？
Ｎ
Ｙ
レコード暗号化キー(ＲＫ)をＤＢカードに書込み
Ｂ１１
モバイルDB名対応のマスタDB名によるマスタDBのファイル読出し
Ｂ１２
レコード抽出条件に基づいてレコード抽出
Ｂ１３
抽出対象フィールドに基づいてレコード構成変更
Ｂ１４
3
2
1

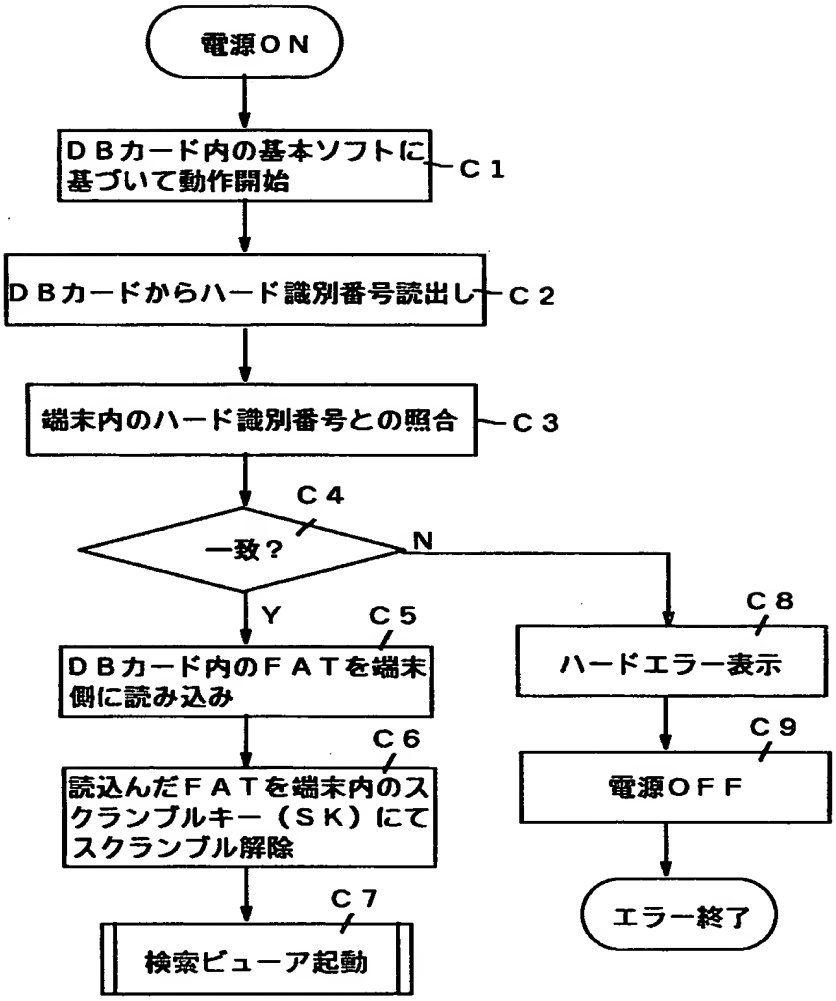
【図１１】


3
2
1
レコード構成の変更された各レコードをレコード暗号化キー（ＲＫ）で暗号化
Ｂ１５
暗号化したレコードによるモバイルＤＢファイルの作成
Ｂ１６
Ｂ１７
他のモバイルDB名有り?
Y
N
テーブル内のカスタマイズＡＰの読出し
Ｂ１８
Ｂ１９
ＤＢカード内に対応カスタマイズＡＰ有り?
N
Y
Ｂ２０
DBカード内の対応APの更新日付と読み出したAPの更新日付は一致?
N
Y
Ｂ２４
読み出したカスタマイズAPをDBカードに上書き
Ｂ２１
他のカスタマイズAP有り?
Y
N
ＤＢカード内の各ファイルの位置を管理するＦＡＴをスクランブルキー（ＳＫ）でスクランブル化
Ｂ２２
Ｂ２３
他のDBカード有り?
N
Y
終　了

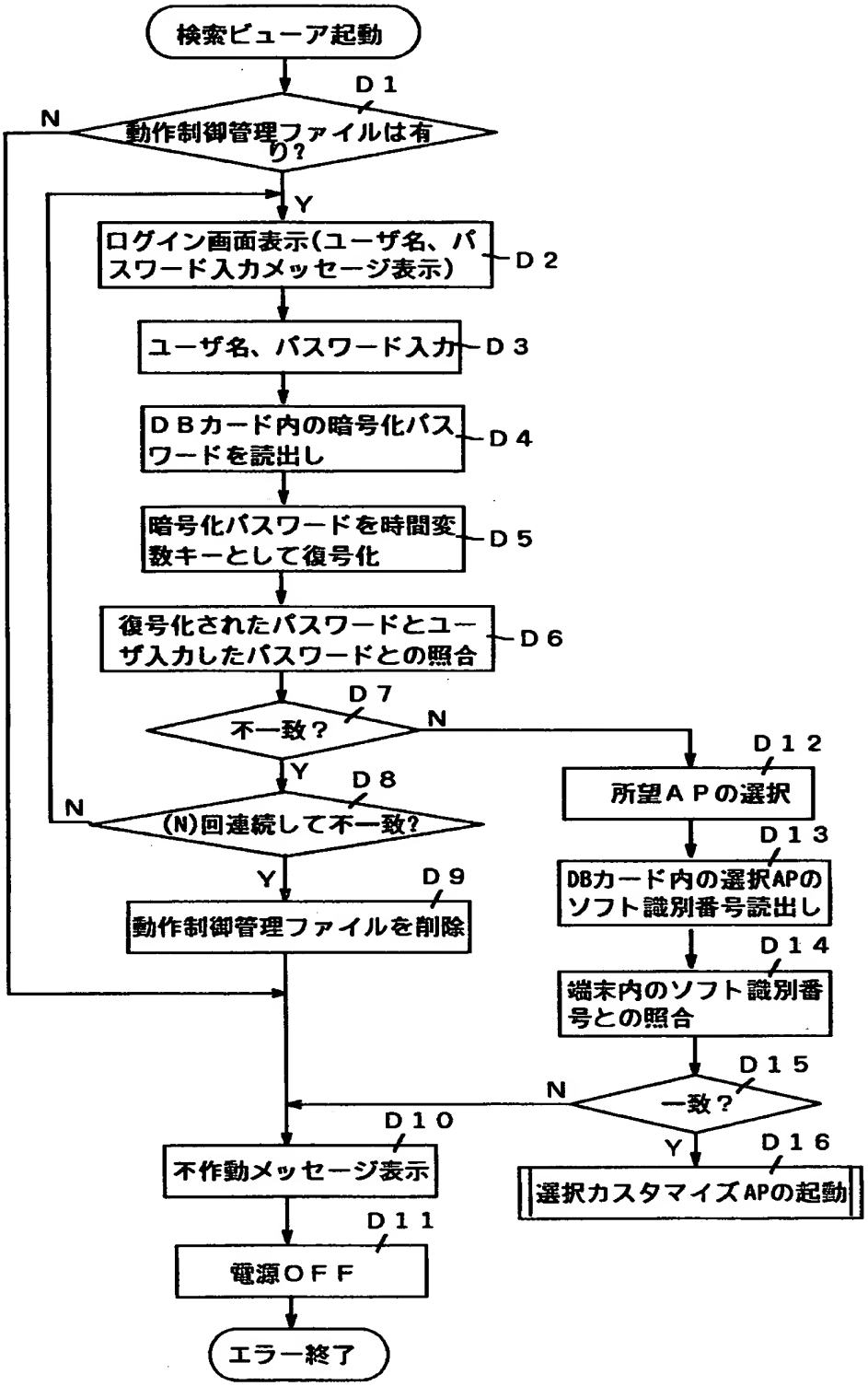
【図１２】


マスタＤＢ
A B C D E F G H
1 2 3 4 5 6 7 8 9 10
(A)
レコード抽出
A B C D E F G H
1 2 3 4 5
(B)
レコード構成変更
A B E G
1 2 3 4 5
(C)
モバイルＤＢの完成

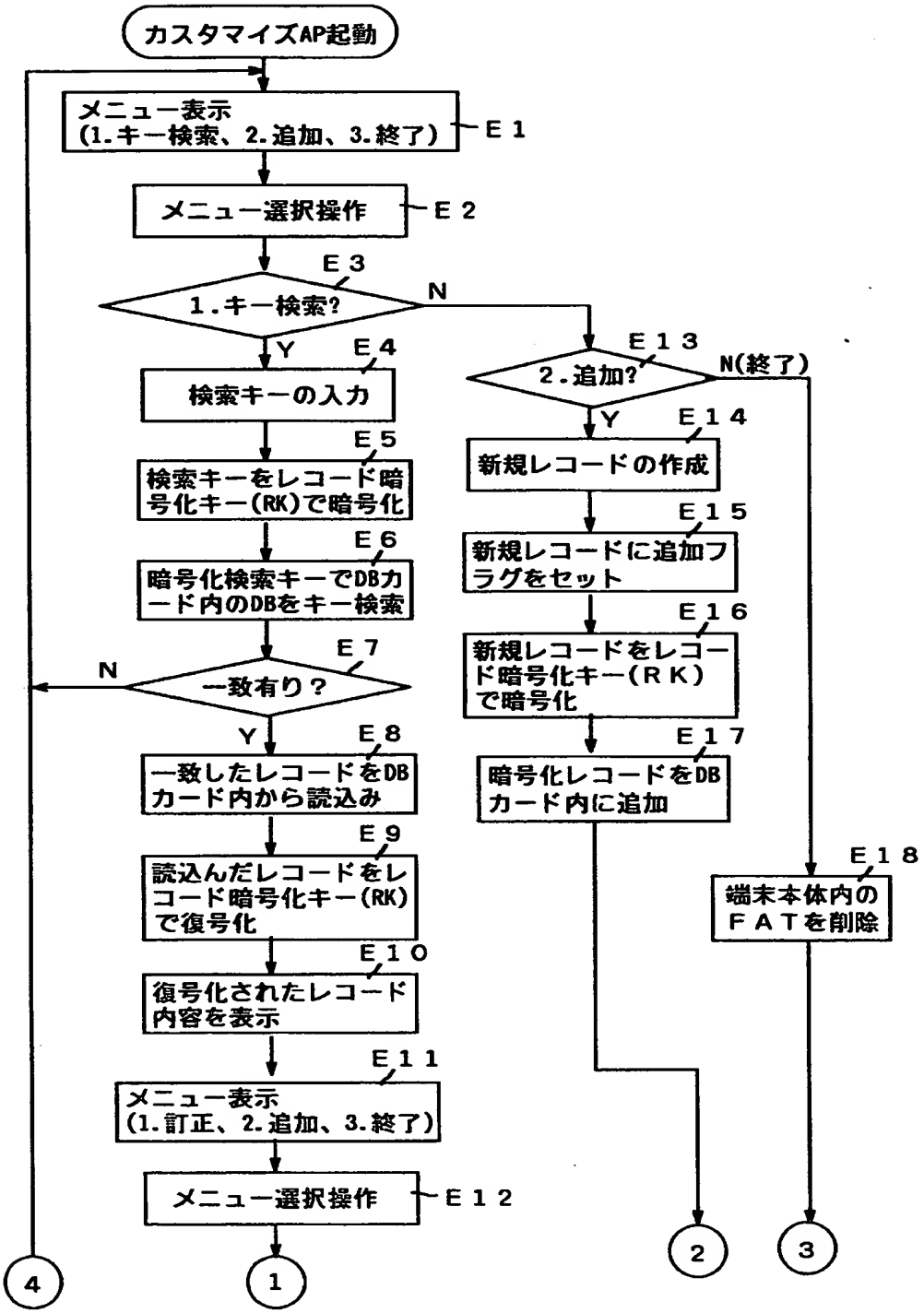
【図１３】


電源ＯＮ
ＤＢカード内の基本ソフトに基づいて動作開始
Ｃ１
ＤＢカードからハード識別番号読出し
Ｃ２
端末内のハード識別番号との照合
Ｃ３
Ｃ４
一致？
Ｎ
Ｙ
Ｃ５
ＤＢカード内のＦＡＴを端末側に読み込み
Ｃ６
読込んだＦＡＴを端末内のスクランブルキー（ＳＫ）にてスクランブル解除
Ｃ７
検索ビューア起動
Ｃ８
ハードエラー表示
Ｃ９
電源ＯＦＦ
エラー終了

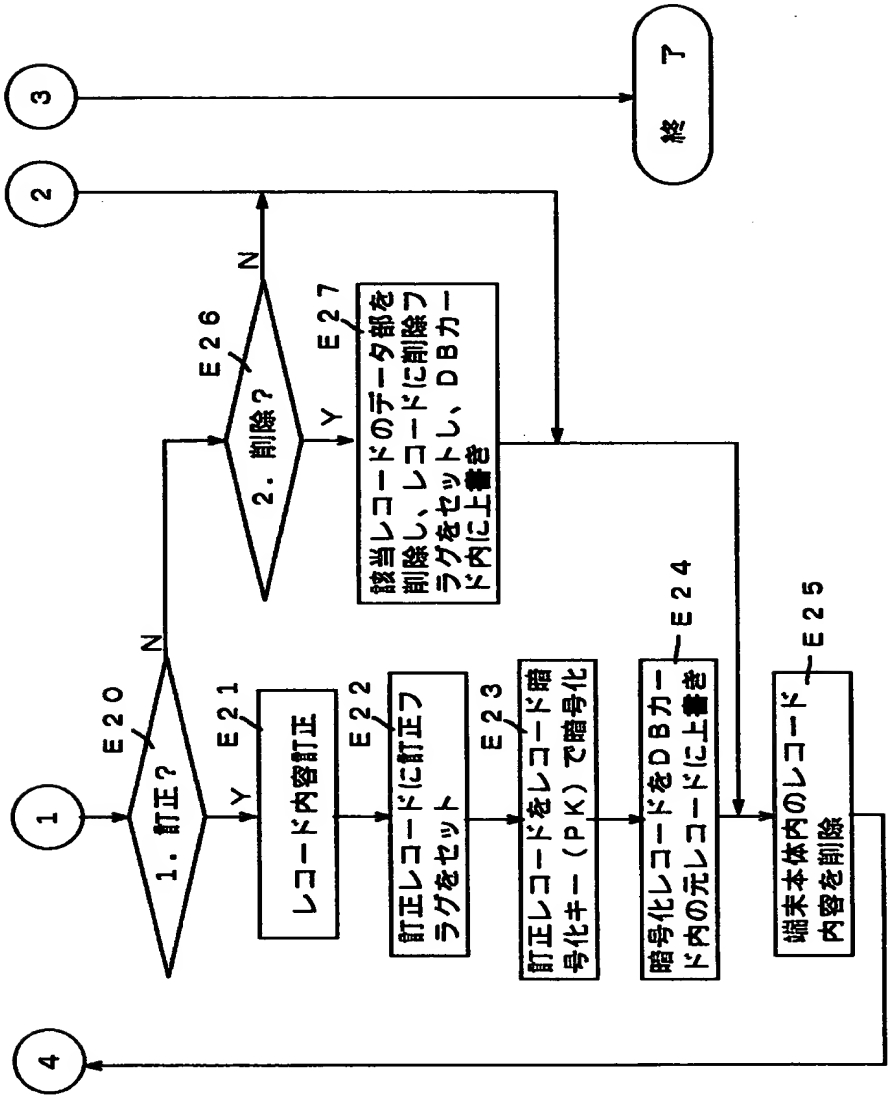
【図１４】


検索ビューア起動
D１
動作制御管理ファイルは有り?
N
Y
ログイン画面表示(ユーザ名、パスワード入力メッセージ表示)
D２
ユーザ名、パスワード入力
D３
ＤＢカード内の暗号化パスワードを読出し
D４
暗号化パスワードを時間変数キーとして復号化
D５
復号化されたパスワードとユーザ入力したパスワードとの照合
D６
D７
不一致？
N
Y
D８
(N)回連続して不一致?
N
Y
D９
動作制御管理ファイルを削除
D１２
所望ＡＰの選択
D１３
DBカード内の選択APのソフト識別番号読出し
D１４
端末内のソフト識別番号との照合
D１５
一致？
N
Y
D１０
不作動メッセージ表示
D１１
電源ＯＦＦ
エラー終了
D１６
選択カスタマイズAPの起動

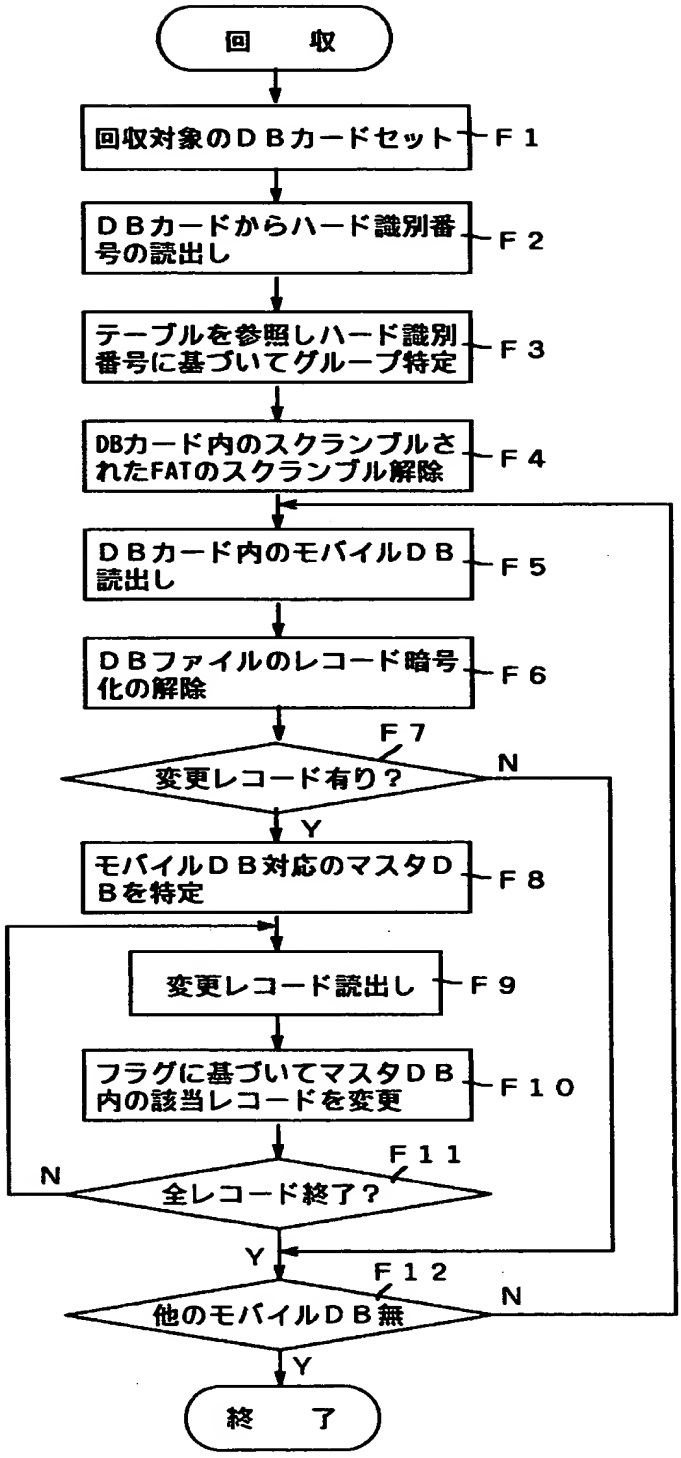
【図１５】


カスタマイズAP起動
メニュー表示
(1.キー検索、2.追加、3.終了)
E１
メニュー選択操作
E２
E３
1.キー検索?
N
Y
E４
検索キーの入力
E５
検索キーをレコード暗号化キー(RK)で暗号化
E６
暗号化検索キーでDBカード内のDBをキー検索
E７
一致有り?
N
Y
E８
一致したレコードをDBカード内から読込み
E９
読込んだレコードをレコード暗号化キー(RK)で復号化
E１０
復号化されたレコード内容を表示
E１１
メニュー表示
(1.訂正、2.追加、3.終了)
メニュー選択操作
E１２
E１３
2.追加?
N(終了)
Y
E１４
新規レコードの作成
E１５
新規レコードに追加フラグをセット
E１６
新規レコードをレコード暗号化キー(ＲＫ)で暗号化
E１７
暗号化レコードをDBカード内に追加
E１８
端末本体内のＦＡＴを削除
1
2
3
4

【図１６】


1
2
3
4
終了
E20
1．訂正？
Y
N
E21
レコード内容訂正
E22
訂正レコードに訂正フラグをセット
E23
訂正レコードをレコード暗号化キー（ＰＫ）で暗号化
E24
暗号化レコードをＤＢカード内の元レコードに上書き
E25
端末本体内のレコード内容を削除
E26
2．削除？
Y
N
E27
該当レコードのデータ部を削除し、レコードに削除フラグをセットし、ＤＢカード内に上書き

【図１７】


回　収
回収対象のＤＢカードセット
Ｆ１
ＤＢカードからハード識別番号の読出し
Ｆ２
テーブルを参照しハード識別番号に基づいてグループ特定
Ｆ３
DBカード内のスクランブルされたFATのスクランブル解除
Ｆ４
ＤＢカード内のモバイルＤＢ読出し
Ｆ５
ＤＢファイルのレコード暗号化の解除
Ｆ６
Ｆ７
変更レコード有り？
N
Y
モバイルＤＢ対応のマスタＤＢを特定
Ｆ８
変更レコード読出し
Ｆ９
フラグに基づいてマスタＤＢ内の該当レコードを変更
Ｆ１０
Ｆ１１
N
全レコード終了？
Y
Ｆ１２
他のモバイルＤＢ無
N
Y
終　了

【書類名】　　要約書

【要約】

【課題】ＤＢカード内のモバイルＤＢをアクセスする場合でも、そのＤＢが暗号化されたままの状態で行うことができ、カードの紛失、盗難あるいは悪意等において、仮に、正当な端末以外がモバイルＤＢのアクセスまでたどり着いた最悪のケースでも、復号化されたレコードのみのセキュリティが問題になるだけで、そのＤＢの全貌が解読される危険性はなく、重要情報の漏洩を確実に防止する。

【解決手段】サーバ装置１は、ＤＢカード３に配布すべきモバイルＤＢの各レコードを個別に暗号化して当該カードに書き込み、携帯端末装置２は、それにセットされているカードが当該端末に対応付けられている正当な媒体かを判別し、端末対応の媒体であれば、そのカード内のＤＢへのアクセスを許可すると共に、アクセス対象として任意に指定されたレコードを個別に読み込み、この１レコード分のデータを復号化してそのレコード内容を表示出力させる。

【選択図】　　図1

認定・付加情報

特許出願の番号	特願２０００－００４２７２
受付番号	５００００２１９３３
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１２年　１月１４日

＜認定情報・付加情報＞

【提出日】	平成12年 1月13日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００１４４３〕

１．変更年月日　　１９９８年　１月　９日
［変更理由］　住所変更
住　所　　東京都渋谷区本町１丁目６番２号
氏　名　　カシオ計算機株式会社